ViPNet Coordinator HW/VA 3.3

Administratorhandbuch

Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Coordinator HW/VA. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Coordinator HW/VA finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Copyright

Version: 00079-06 32 01 DEU

Marken

Wie Sie Infotecs erreichen

Oberwallstr. 24

10117 Berlin

Deutschland

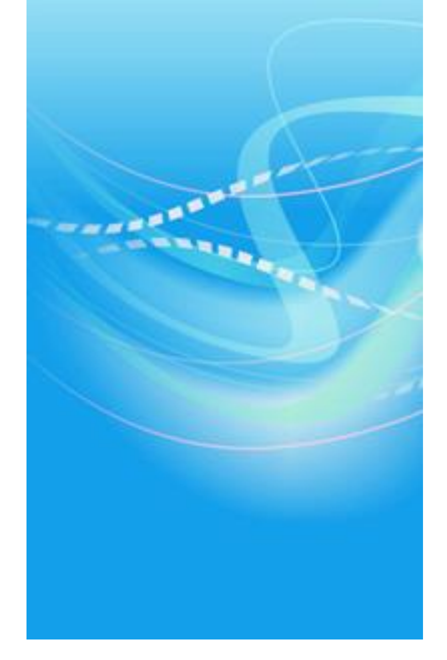
Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.de

Inhalt



Einführung

Über dieses Dokument

Dieses Dokument bildet den Anhang zum Hauptdokument „ViPNet Coordinator HW/VA. Administratorhandbuch“ und enthält Beschreibungen und Beispiele für Befehle, die durch Befehlszeilenschnittstelle für Konfiguration des ViPNet Coordinator HW/VA angegeben werden sollen. Für die erfolgreiche Arbeit mit diesem Dokument ist es empfehlenswert, dass der Leser über Grundlagenwissen in Netzwerktechnologie sowie über erste Einblicke in die ViPNet-Technologie verfügt. Ausführliche Informationen über ViPNet-Netzwerke s. Dokumente „ViPNet VPN. Benutzerhandbuch“ und „Die Technologie von ViPNet. Allgemeine Informationen“.

Zielgruppe

Dieses Dokument wendet sich an Administratoren von ViPNet VPN Netzwerken, die für die Einrichtung und Einstellung von ViPNet Coordinator HW/VA zuständig sind. Das vorliegende Handbuch enthält eine allgemeine Beschreibung von ViPNet Coordinator HW/VA und kurze Anweisungen zur dessen Einrichtung und Benutzung in gebräuchlichen Verwendungsszenarios. Das hilft Ihnen den ViPNet Coordinator HW/VA schnell einzurichten, ohne sich dabei an die vollständige Version des Administratorhandbuchs zu wenden. Um mit dem vorliegenden Buch erfolgreich zu arbeiten, sollte der Leser Grundkenntnisse in Netzwerktechnologien und Erfahrungen mit der ViPNet Software-Lösungen haben. Ausführliche Informationen über ViPNet Netzwerke finden Sie in „ViPNet VPN. Benutzerhandbuch“.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
⚠	**Achtung!** Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
ℹ	**Hinweis.** Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.

Symbol	Beschreibung
	Tipp. Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.
Menü > **Untermenü** > **Befehl**	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsleiste.
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Für die Beschreibung der Befehle werden in diesem Dokument folgende Konventionen verwendet:

- Befehle, die aussschließlich im Administratormodus ausgeführt werden können, werden in roter Farbe hervorgehoben. Beispiel:

  ```
  Befehl
  ```

- Parameter, die vom Benutzer festgelegt werden sollen, werden in Pfeilklammern eingeschlossen angezeigt. Beispiel:

  ```
  Befehl <Parameter>
  ```

- Optionale Parameter werden durch eckige Klammern begrenzt angezeigt. Beispiel:

  ```
  Befehl <obligatorischer Parameter> [optionaler Parameter]
  ```

- Wenn bei der Befehlseingabe ein Parameter aus mehreren möglichen Parameteroptionen ausgewählt werden soll, werden die Parameteroptionen in geschwungenen Klammern durch Strich getrennt angezeigt. Beispiel:

  ```
  Befehl {Option-1 | Option-2}
  ```

Kurzleitfaden

Tabelle 3. Kurzübersicht über die Dokumentabschnitte

	Verweis
Erste Schritte	Installation von ViPNet Coordinator HW/VA (auf S. 28) Zugreifen auf ViPNet Coordinator HW/VA (auf S. 43)
Konfiguration des Knotens	Konfiguration der Systemparameter (auf S. 52) ViPNet Coordinator HW/VA zum Netzwerk verbinden (auf S. 60) Zuverlässiger Zugang zu Netzwerkressourcen durch Verwendung alternativer Traffic-Kanäle (auf S. 119) Failover-System (auf S. 127)
Konfiguration der integrierten Dienste	Konfiguration der integrierten Dienste • Parameter des Wi-Fi-Access Points einstellen (auf S. 82) • Parameter des DHCP-Servers einstellen (auf S. 84) • Parameter des DNS-Servers einstellen (auf S. 85) • Parameter des NTP-Servers einstellen (auf S. 86) Konfiguration des Proxy-Servers (auf S. 89) Konfiguration des VoIP-Servers (auf S. 98) Konfiguration des IPsec-Gateways (auf S. 103) Konfiguration der integrierten Firewall (auf S. 105)
Bereitsstellungsszenarien	ViPNet Coordinator HW/VA für Einrichtung des lokalen Netzwerks verwenden (auf S. 135) Zentralisierten Proxyserver verwenden (auf S. 144) ViPNet Coordinator HW/VA für Einrichtung des lokalen Netzwerks verwenden (auf S. 135) Bereitstellung eines sicheren Zugangs zum Firmen-LAN von mobilen Geräten über IPsec-Kanäle (auf S. 152) Bereitstellung eines sicheren Zugangs zu Ressourcen im Firmen-LAN aus Remote-Netzwerkknoten (Client-to-Site Verbindung) (auf S. 147)

Über ViPNet Coordinator HW/VA

ViPNet Coordinator HW/VA stellt eine Softwarelösung auf Basis des Betriebssystems Linux dar und ist dafür bestimmt, im geschützten ViPNet VPN-Netzwerk die Funktionen eines Servers – des Coordinators zu erfüllen (s. Funktionen eines Coordinators im privaten ViPNet Netzwerk auf S. 25). ViPNet Coordinator HW/VA unterstützt eine Vielzahl an Plattformen mit unterschiedlichen verfügbaren Features.

Unterstützte ViPNet Coordinator HW/VA-Plattformen

ViPNet Coordinator HW/VA unterstützt die folgenden Plattformen:

- ViPNet Coordinator HW Hardware-Appliances:
  - HW100-Serie: kompakte Geräte für den Einsatz in Büro-VPNs mittlerer Größe, bereitgestellt als Standalone-Computer in allgemein zugänglichen Büroräumlichkeiten.
  - HW1000-Serie: Geräte für den Einsatz in großen und extragroßen Unternehmens-VPN, bereitgestellt in speziellen Serverräumen in Serverracks.
- ViPNet Coordinator VA virtuelle Geräte für den Einsatz in virtuellen Umgebungen.

  Die Kapazitäten eines virtuellen Geräts sind durch seine Lizenz begrenzt. Die Gerätelizenzen für VA100, VA1000 und VA2000 stellen Features bereit, die den Features der analogen Hardware-Appliances HW100, HW1000 und HW2000 entsprechen.

Hinweis. Im Hinblick auf einige weniger wichtige Kapazitäten einer Hardware-Appliance kann es Unterschiede zu den entsprechenden Features der virtuellen Appliance geben. Die Details zu den Lizenzeinschränkungen finden Sie in den nachfolgenden Abschnitten.

ViPNet Coordinator HW100 Hardware-Appliances

Tabelle 4. ViPNet Coordinator HW100-Ausführungen

	HW100 X1	HW100 X2	HW100 X4	HW100 X5	HW100 X6
Physische Parameter					
Formfaktor	Standalone -Computer	Standalone -Computer	Standalone -Computer	Standalone-Computer	Standalone -Computer

	HW100 X1	HW100 X2	HW100 X4	HW100 X5	HW100 X6
Größe, mm (L x W x H)	130 x 187 x 73	130 x 187 x 73	85 x 135 x 30	85 x 135 x 30	85 x 135 x 30
Gewicht, kg	1.6	1.6	0.5	0.5	0.5
Stromversorgung	60 W	60 W	30 W	30 W	30 W
Allgemeine Kapazitäten					
Prozessor	Intel Atom, 2 core	Intel Atom, 2 core	Intel Atom, 4 core	Intel Atom, 4 core	Intel Atom, 4 core
RAM (min), GB	1	1	2	2	2
Festplattenspeicher (min), GB	2	80	2	2	2
USB-Ports	2	2	2	2	2
Andere Ports	VGA	VGA	HDMI, COM	HDMI, COM	HDMI, COM
Netzwerkadapter					
Ethernet	4x 1 Gbit/s	4x 1 Gbit/s	3x 1 Gbit/s	3x 1 Gbit/s	3x 1 Gbit/s
Wi-Fi	kein	kein	kein	wird integriert	kein
3G/LTE-Modem	Externes USB-Gerät (nicht im Distributionskit erhalten)				3G

Hinweis. Die folgenden Features werden von ViPNet Coordinator HW der Modifikationen HW 100 X1/X4/X5/X6 nicht unterstützt:

- Hinzufügen von VPN-Clients. In einem VPN können diese Appliances ausschließlich Verbindungen mit offenen Knoten tunneln.
- Proxyserver-Funktionen (s. Konfiguration des Proxy-Servers auf S. 89) inklusive Antivirus und Inhaltsfilter.
- Speichervergrößerung durch Auslagerung (s. Konfiguration der Auslagerungsdatei auf S. 55).

Failover-System im Cluster-Modus (s. Failover-System auf S. 127) ist für Coordinator HW-Modifikationen nicht verfügbar.

ViPNet Coordinator HW1000 Hardware-Appliances

Tabelle 5. ViPNet Coordinator HW1000 D1-Ausführungen

Physische Parameter	
Formfaktor	Rack-Mount-Server
Größe, mm (L x W x H)	434 x 394,3 x 42,4
Gewicht, kg	8.058
Stromversorgung	250 W
Allgemeine Kapazitäten	
Prozessor	Intel Xeon E3-1270 v3
RAM (min), GB	8
Festplattenspeicher (min), GB	2x 300 GB
USB-Ports	2x USB 2.0, 2x USB 3.0
Andere Ports	VGA, COM
Netzwerkadapter	
Ethernet	2x 1 Gbit/s
Wi-Fi	kein

ViPNet Coordinator VA - virtuelle Appliances

Tabelle 6. ViPNet Coordinator VA-Ausführungen

	VA 100	VA 1000	VA 2000
Anzahl der Verkehrsverarbeitungs Kernel-Threads	2	8	16
Netzwerkadapter			
Ethernet	4 Ports	4 Ports	4 Ports
Wi-Fi, 3G/LTE-Modem	kein	kein	kein

Hauptfeatures

Die wichtigsten Features von ViPNet Coordinator HW/VA sind in der nachfolgenden Tabelle aufgelistet.

Hinweis. Manche Features sind nur für bestimmte unterstützte Plattformen verfügbar (s. Unterstützte ViPNet Coordinator HW/VA-Plattformen auf S. 12).

Tabelle 7. Features des ViPNet Coordinator HW/VA

Feature	Unterstützung
Netzwerk	
Konnektivität	Ethernet, Wi-Fi, 3G/LTE
Wi-Fi-Zugriffspunkt	Wird unterstützt
VPN	ViPNet VPN: erweiterte Point-to-Multipoint VPN-Technologie.
	IPsec: IKEV1 Site-to-Site, Client-to-Site.
Statisches Routing	Wird unterstützt
Stateful Firewall	Wird unterstützt
NAT	Wird unterstützt
Verwendung alternativer Datenübertragungskanäle	Zwei Modi: Redundanzmodus, Lastenausgleich
Dienste	
DHCP	Client, Server
DNS	Server
NTP	Server
Proxyserver	HTTP, HTTPS
Proxyinhaltskontrolle (Proxy Content Control)	Wird unterstützt
Proxy-Antivirusfilterung	ClamAV
VoIP	SIP-Server
Failover-System	Wird unterstützt (nur Coordinator VA-Plattformen)
Verwaltung von ViPNet Coordinator HW/VA	
Konfiguration	Über die Webschnittstelle
	Über die Befehlszeilenschnittstelle
	Aus dem Programm ViPNet Network Manager

Feature	Unterstützung
SSH	Server
Remote-Softwareupdates	Wird unterstьtzt
Backup	Sicherung und Wiederherstellung der Konfigurationen unter Verwendung eines USB-Datenträgers
Protokollierung (Logdatei)	Syslog, rsyslog (Remote-syslog)
SNMP-Monitoring	Wird unterstützt

Hinweis. Die folgenden Features werden von ViPNet Coordinator HW der Modifikationen HW 100 X1/X4/X5/X6 nicht unterstützt:

- Hinzufügen von VPN-Clients. In einem VPN können diese Appliances ausschließlich Verbindungen mit offenen Knoten tunneln.
- Proxyserver-Funktionen (s. Konfiguration des Proxy-Servers auf S. 89) inklusive Antivirus und Inhaltsfilter.
- Speichervergrößerung durch Auslagerung (s. Konfiguration der Auslagerungsdatei auf S. 55).

Failover-System im Cluster-Modus (s. Failover-System auf S. 127) ist nur für Coordinator VA-Modifikationen verfügbar.

Lieferumfang

Ein ViPNet Coordinator HW/VA Distributionskit umfasst:

- Abhängig vom Formfaktor der Appliance:
    - bei ViPNet Coordinator HW-Ausführungen die ViPNet Coordinator HW Appliance.
    - bei ViPNet Coordinator VA-Ausführungen die Bereitstellungsdatei der virtuellen Appliance (`coordinatorhw_vipnet_x.x-xxx.ova`).

      Diese Datei wird auch für die Bereitstellung beliebiger Ausführungen von ViPNet Coordinator VA verwendet.
- Die Dateien für Upgrade der ViPNet Coordinator HW/VA-Software.
    - Die Software-Upgrade-Datei `coordinatorhw_vipnet_driv_x.x-xxx.lzh`, die für das Upgrade auf der Version 3.2 verwendet werden.
    - Die Konfigurationsdatei für das Software-Upgrade `hwinit-x.x-xxx_upgrade.xml`.
- Dokumente im PDF-Format, nämlich:

- „ViPNet Coordinator HW/VA. Administratorhandbuch“ als PDF-Datei.
- „ViPNet Coordinator HW/VA. Failover-System“ als PDF-Datei.
- „ViPNet Coordinator HW/VA. Referenzhandbuch“ als PDF-Datei.

Systemanforderungen

Anforderungen für die Verwendung von ViPNet Coordinator HW/VA:

- Verwenden Sie für den lokalen Zugriff auf eine Hardware-Appliance (s. Verwalten von ViPNet Coordinator HW/VA-Knoten auf S. 46) die folgenden Geräte:
  - Monitor,
  - USB-Tastatur.
- Folgende virtuelle Umgebungen können für die Bereitstellung einer virtuellen Appliance verwendet werden:
  - VMware Workstation,
  - VMware vSphere,
  - Oracle Virtual Box.
- Das Programm ViPNet Network Manager sollte die Version 4.2 oder höher besitzen.
- Unterstützte 3G/LTE USB-Modems:
  - 3G Huawei K3772 (Vodafone),
  - 3G Huawei E303 (Vodafone),
  - LTE Huawei E398 (Deutsche Telekom Speedstick LTE III).

Neue Möglichkeiten der Version 3.3

In der Version 3.3 wurde die HW1000 D1 Hardware-Plattform hinzugefügt, einige kleinere Fehler wurden korrigiert.

Kontakt

FAQ und andere Hilfsinformation

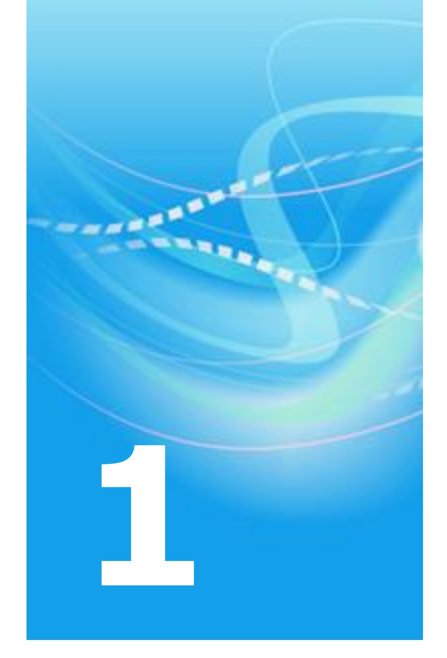
Informationen über ViPNet-Produkte und Lösungen, gängige Fragen und andere nützliche Hinweise sind auf der Webseite von „InfoTeCS“ zusammengefasst. Unter den aufgeführten Links können Sie zahlreiche Antworten auf mögliche während des Produktbetriebs auftretenden Fragen finden.

- Allgemeine Geschäftsbedingungen http://www.infotecs.de/about/terms.php
- ViPNet-Lösungen im Überblick http://www.infotecs.de/solutions/
- Frequently Asked Questions http://www.infotecs.biz/doc_vipnet/DEU/index.htm#2_11572.htm
- ViPNet-Wissensdatenbank http://www.infotecs.biz/doc_vipnet/DEU/index.htm#1_main.htm

Kontakt

Bei Fragen zur Nutzung von ViPNet-Software sowie möglichen Wünschen und Anregungen nehmen Sie Kontakt mit den Mitarbeitern der Firma „InfoTeCS GmbH“ auf. Für die Lösung aufgetretener Problemfälle wenden Sie sich an den technischen Support.

- E-Mail: support@infotecs.de.
- Anfrage an den technischen Support via Internetseite http://infotecs.de/support/
- Support Hotline +49 (0) 30 206 43 66 22 (Tel.); +49 (0) 30 206 43 66 66 (Fax).



Übersicht

Zweck und Einsatzbereich von ViPNet Coordinator HW/VA

Das Appliance ViPNet Coordinator HW/VA wird als Bestandteil der Softwarelösung ViPNet VPN eingesetzt, die dafür konzipiert ist, virtuelle private Netzwerke (s. Geschützte ViPNet Netzwerk auf S. 24) einzurichten und zu verwalten. Dies ist eine integrierte Lösung, die Verbindungen zu Unternehmensnetzwerken, Remotebenutzern, mobilen Benutzern, Niederlassungen und Geschäftspartnern unter Verwendung einer Vielzahl von offenen Plattformen und Sicherheits-Appliances ermöglicht. Der Schutz von Daten, die über öffentliche Netzwerke übertragen werden, wird mit Hilfe von Trafficverschlüsselung, Authentisierung von Netzwerkknoten und Zugangskontrolle sichergestellt.

ViPNet Coordinator HW/VA stellt das System auf Basis einer adaptierten Version des Linux-Betriebssystems mit den ViPNet Diensten dar und unterstütz verschiedene ViPNet Dienste. Grundlegende Funktionen von ViPNet Coordinator HW/VA

- VPN-Server, der eingehende geschützte Verbindungen zusammenfasst. ViPNet Coordinator HW/VA unterstützt die ViPNet Technologie, die direkte Verbindungen zwischen den Knoten nach dem Client-to-Client-Schema (s. Geschützte ViPNet Netzwerk auf S. 24) ermöglicht, sowie die IPsec-Technologie (s. IPsec-Protokoll auf S. 245).

  Ebenso ist die Einrichtung eines abgesicherten Kanals zwischen den ViPNet und den IPsec-Netzwerken möglich (site-to-site) (s. Bereitstellung eines sicheren Zugangs zu Ressourcen im Firmen-LAN aus anderen LANs (Site-to-Site Verbindung) auf S. 159).

- Firewall, die alle grundlegenden Parameter und Statuswerte von Netzwerkverbindungen überwacht. ViPNet Coordinator HW/VA erlaubt es, für jeden Netzwerkadapter des Computers Filterregeln für IP-Pakete nach Protokoll, IP-Adresse oder Port einzustellen (s. Regeln zur Filterung des Traffics auf S. 112).

  Außerdem führt ViPNet Coordinator HW/VA die Übersetzung von IP-Adressen (NAT) durch (s. Regeln der Adressenübersetzung auf S. 114).

- VPN-Gateway (Tunnelender Server), der die Organisation von abgesicherten Zugängen zu tunnelierten Firmenressourcen ermöglicht (s. Bereitstellung eines sicheren Zugangs zu Ressourcen im Firmen-LAN aus Remote-Netzwerkknoten (Client-to-Site Verbindung) auf S. 147).

ViPNet Coordinator HW/VA kann auch zusätzliche Funktionen übernehmen:

- Den Betrieb der Netzwerkdienste DHCP, DNS und NTP sichern (s. Parameter für Netzwerkdienste einstellen auf S. 82);
- Als Proxyserver (s. Konfiguration des Proxy-Servers auf S. 89) mit Kontroll- und Antiviren-Prüffunktionen eingesetzt werden;
- Als VoIP-Server (s. Konfiguration des VoIP-Servers auf S. 98) auftreten, der die Installation eines firmeninternen IP-Telefoniesystemes ermöglicht.

Die grundlegenden Einsatzmöglichkeiten von ViPNet Coordinator HW/VA in Firmennetzwerken werden im Abschnitt Verwendungsszenarien für ViPNet Coordinator HW/VA (auf S. 134) beschrieben.

Komponente

Folgende grundlegende funktionelle Module bilden den Inhalt von ViPNet Coordinator HW/VA:

- **Kernel-Level-Netzwerkschutztreiber ViPNet**, der unmittelbar mit anderen Netzwerkkartentreibern interagiert und den gesamten Datenaustausch des Computers mit dem externen Netzwerk überwacht.
- **Steuerungsprogramm**, das die benötigten Parameter für den ViPNet Treiber lädt, Informationen über die IP-Adressen von Clients sendet und empfängt, den Traffic protokolliert, usw. Es wird empfohlen, dieses Programm immer laufen zu lassen. Beim Beenden des Programms arbeitet der ViPNet Treiber aber weiter, der Datenaustausch wird nicht unterbrochen.
- **Crypto-Treiber**, der kryptografische Operationen auf Anfrage des Treibers iplir ausführt.
- **Failover-System**, das Treiber und ein spezielle Daemon enthält. Der Treiber arbeitet auf einer sehr niedrigen Schicht und bleibt in den meisten Fällen auch dann funktionsfähig, wenn das System auf externe Ereignisse nicht mehr reagiert.
- **MFTP-Trasportmodul**, der den Empfang und die Weiterleitung von Transportdateien zwischen den ViPNet Netzwerkknoten gewährleistet.
- **Befehlszeileninterpreter**, mit dessen Hilfe die integrierte Hard- und Softwarelösung administriert wird.
- **DHCP-Server**, der für die dynamische Vergabe von IP-Adressen an DHCP-Clients sorgt.
- **DNS-Server**, der die Auflösung von Namen in IP-Adressen gewährleistet.
- **NTP-Server**, mit dessen Hilfe die Synchronisation der Systemzeit erfolgt.
- **Proxyserver** mit der Möglichkeit zur Kontrolle und Antivirus-Überprüfung des Inhalts von Internetobjekten.
- **VoIP-Server**, mit dessen Hilfe ein firmeninternes IP-Telefoniesystem eingerichtet werden kann.

Geschützte ViPNet Netzwerk

Das Appliance ViPNet Coordinator HW/VA ist dafür konzipiert, in einem geschützten ViPNet Netzwerk, das auf Basis der Software-Lösung ViPNet VPN eingerichtet wurde, eingesetzt zu werden.

Das ViPNet Netzwerk stellt ein virtuelles geschütztes Netzwerk (s. Virtuelles Privates Netzwerk (VPN) auf S. 247) dar, das über bestehende lokale oder globale Netzwerke beliebiger Struktur installiert werden kann. Im Unterschied zu vielen gängigen VPN-Lösungen gewährleistet die ViPNet Technologie eine abgesicherte Interaktion zwischen den Netzwerkknoten (s. ViPNet Netzwerkknoten auf S. 247) nach dem „Client-to-Client“-Schema.

Der Schutz von Daten wird innerhalb des ViPNet Netzwerks mit Hilfe einer speziellen Software sichergestellt, die zwei grundlegende Funktionen erfüllt:

- Filterung des gesamten IP-Traffics der Netzwerkknoten. Die Traffic-Filterung erfolg in Übereinstimmung mit vordefinierten Sicherheitsstufen (auf S. 26) und Benutzerregeln.
- Verschlüsselung von Verbindungen zwischen den ViPNet Netzwerkknoten. Für die Verschlüsselung des Traffics werden symmetrische Schlüssel verwendet, die zentralisiert angelegt und verteilt werden.

Für die Administration des geschützten ViPNet Netzwerks wird das Programm ViPNet Network Manager (auf S. 247) verwendet. Mit Hilfe von ViPNet Network Manager werden neue Netzwerkknoten angelegt, Verbindungen zwischen diesen Knoten definiert, Parameter einzelner Knoten konfiguriert, Schlüssel für jeden Knoten erstellt und zentralisierte Updates von Software und Schlüssel auf den Knoten durchgeführt.

ViPNet Netzwerkknoten werden in zwei Typen unterteilt:

- Clients: Arbeitsstationen der Benutzer im ViPNet Netzwerk. Auf den Clients sollte die Software ViPNet Client installiert sein.
- Coordinatoren (s. Coordinator (ViPNet Coordinator) auf S. 242): Servern des ViPNet Netzwerks (s. Funktionen eines Coordinators im privaten ViPNet Netzwerk auf S. 25). Ein Netzwerkknoten mit installiertem ViPNet Coordinator HW/VA-Appliance.

Ein ViPNet Netzwerk kann auch folgende Elemente umfassen:

- Computer im lokalen Netzwerk, auf denen keine ViPNet Software installiert ist, die jedoch durch die Technologie der Tunneling (s. Tunnelung auf S. 247) geschützt sind. Diese Computer werden als „getunnelte Knoten“ bezeichnet und von ViPNet Coordinatoren getunnelt, die eine Verbindung dieser Knoten mit anderen Netzwerken (z. B. mit dem Internet) gewährleisten.

- Mobile Geräte, die über das IPsec-Protokoll mit dem ViPNet Netzwerk verbunden sind (s. Bereitstellung eines sicheren Zugangs zum Firmen-LAN von mobilen Geräten über IPsec-Kanäle auf S. 152).

Funktionen eines Coordinators im privaten ViPNet Netzwerk

Ein Coordinator (s. Coordinator (ViPNet Coordinator) auf S. 242) ist ein VPN-Server in einem geschütztem ViPNet Netzwerk. Je nachdem welche Aufgaben im ViPNet Netzwerk benötigt werden, kann ein Coordinator folgende Funktionen erfüllen:

- VPN-Server, der Informationen über den Zustand von ViPNet Netzwerkknoten speichert und diese an seine Clients weiterleitet.

  Jeder Client eines ViPNet Netzwerks teilt seinem VPN-Server in gewissen Zeitabständen seinen Zustand mit. VPN-Server tauschen die von Clients erhaltenen Informationen untereinander aus. Jeder Client des ViPNet-Netzwerks bekommt von seinem VPN-Server Daten über die Zugangsmöglichkeiten zu denjenigen ViPNet Netzwerkknoten, mit denen er verbunden ist, sowie über den Zustand dieser Netzwerkknoten.

- Firewall. Der Coordinator ist dafür zuständig, offene, verschlüsselte und getunnelte IP-Pakete auf jedem Netzwerkadapter nach IP-Adressen, Protokollen und Ports zu filtern.

  Filterungsverfahren für offenen und getunnelten Datenverkehr entsprechen den vorher eingestellten Filterregeln und Sicherheitsstufen (auf S. 26).

  Auch führt der Coordinator die Umsetzung von IP-Adressen (s. Netzwerkadressenübersetzung (NAT) auf S. 245) für verschlüsselten und unverschlüsselten Datenverkehr durch.

  Die Umsetzung von IP-Adressen für verschlüsselten Datenverkehr wird entsprechend den voreingestellten Parametern durchgeführt. Diese Parameter können nicht geändert werden.

  Bei der Umsetzung von IP-Adressen für offenen Datenverkehr ist es möglich, Regeln für die statische und dynamische NAT-Funktion einzustellen. Dadurch werden zwei wichtige Aufgaben gelöst:

  - Verbindung eines lokalen Netzwerks mit Internet, wenn die Anzahl der Knoten im lokalen Netzwerk die Anzahl der vom Provider bereitgestellten öffentlichen IP-Adressen überschreitet.

- Zugang zu lokalen Netzwerkknoten aus dem Internet.

- VPN-Gateway (tunnelender Server). Tunnelung des Datenverkehrs. Coordinatoren können den Datenverkehr von offenen Netzwerkknoten in potenziell gefährdeten Netzwerkbereichen sichern. Das gilt für Computer oder andere Netzwerkgeräte ohne ViPNet Client- oder ViPNet Coordinator-Software.

  Der Datenverkehr von einem getunnelten Netzwerkknoten geht auf einen Coordinator unverschlüsselt ein. Der Coordinator verschlüsselt diesen Datenverkehr und leitet den an den Zielknoten oder ggf. einen anderen Coordinator weiter. Verschlüsselte Daten für einen getunnelten Netzwerkknoten werden durch den Coordinator entschlüsselt und an den Netzwerkknoten weitergeleitet.

- Kommunikationsserver, der Schlüssel- und Softwareupdates, die aus dem Programm ViPNet Network Manager versendet werden, liefert und den Paketaustausch der ViPNet Anwendungen (s. Datei (Transportdatei) auf S. 242) zwischen den Netzwerkknoten gewährleistet.

  Das Routing von Nutzdaten und Steuerungspaketen wird durch das Transportmodul ViPNet MFTP durchgeführt. Es nimmt die Pakete von ViPNet Netzwerkknoten an und leitet sie an den Zielknoten oder an einen anderen Routing Server weiter.

Sicherheitsstufen

ViPNet Security Gateway verfügt über vier vorkonfigurierte Filterungspolicen für offenen Datenverkehr, die als Sicherheitsstufen bezeichnet werden:

1. Alle Verbindungen blockieren.

   Es sind ausschließlich Verbindungen mit geschützten ViPNet Netzwerkknoten (s. Geschützter Netzwerkknoten auf S. 244) erlaubt, alle Verbindungen mit offenen Netzwerkknoten (auch mit getunnelten Knoten) werden blockiert.

2. Nur erlaubte Verbindungen durchlassen.

   Verbindungen mit geschützten ViPNet Netzwerkknoten sind erlaubt. Eine Verbindung mit offenen Netzwerkknoten ist nur dann möglich, wenn sie in Filterregeln explizit erlaubt wurde.

   Es ist empfehlenswert, die zweite Sicherheitsstufe einzustellen. Standardmäßig ist sie auf allen Netzwerkadaptern eines ViPNet Coordinator HW/VA aktiviert.

3. Ausgehende Verbindungen erlauben außer verbotene.

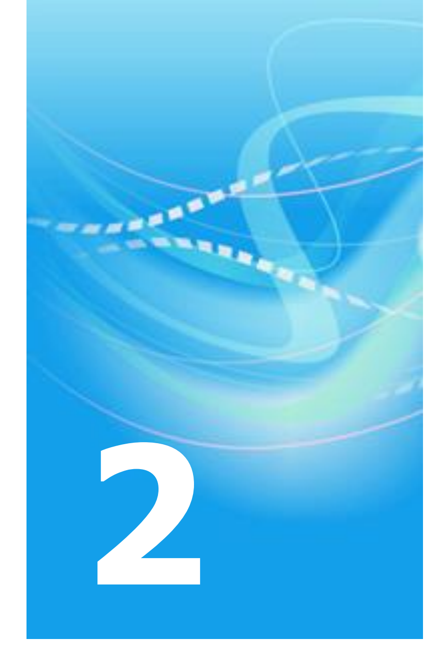
   Verbindungen mit geschützten ViPNet Netzwerkknoten sind erlaubt. Ausgehende Verbindungen mit offenen Netzwerkknoten sind möglich, insofern sie in Filterregeln nicht untersagt worden sind. Eine eingehende Verbindung ist nur dann möglich, wenn sie in Filterregeln explizit erlaubt wurde.

4 Alle Verbindungen erlauben.

Verbindungen mit geschützten ViPNet Netzwerkknoten sind erlaubt. Alle Verbindungen mit offenen Netzwerkknoten sind erlaubt. Filterregeln werden dabei nicht beachtet.

Achtung! Es wird nicht empfohlen, die vierte Sicherheitsstufe auf Netzwerkadaptern eines Coordinators einzustellen, denn in diesem Fall ist der Coordinator vor einen unbefugten Zugriff nicht geschützt.

Verwenden Sie diese Sicherheitsstufe nur für den Reservekanal in einem Failover-Cluster (s. Zweckbestimmung des Failover-Systems auf S. 128) oder kurzfristig für Testzwecke.



Installation von ViPNet Coordinator HW/VA

Vorgehensweise bei der Installation von ViPNet Coordinator HW/VA

Sie können die Software auf die Version 3.2 aktualisieren (s. Upgrade der Software auf ViPNet Coordinator HW/VA auf S. 30), wenn Sie eine vorherige Version benutzen. Führen Sie die Aufgaben in der folgenden Tabelle, wenn Sie die ViPNet Coordinator HW/VA-Software neu installieren möchten.

Tabelle 8. Vorgehensweise bei der Installation von ViPNet Coordinator HW/VA

	Aktion	Verweis
☐	Erwerben oder aktualisieren Sie Ihre ViPNet VPN-Lizenz (s. Lizenzerweiterung für ViPNet VPN auf S. 245), sodass die Verwendung von ViPNet Coordinator HW/VA möglich ist.	Kontaktieren Sie einen Vertreter von Infotecs.
☐	Wenn Sie einen ViPNet Coordinator VA installieren, dann stellen Sie die Imagedatei der virtuellen Appliance `*.ova` in Ihrer virtuellen Umgebung bereit.	Folgen Sie den Richtlinien der Umgebungssoftware.
☐	Erstellen Sie einen neuen Coordinator im Programm ViPNet Network Manager und nehmen alle notwendigen Einstellungen vor. Erstellen Sie einen Schlüsseldistribution.	ViPNet Coordinator HW/VA im ViPNet Network Manager einstellen (auf S. 33)
☐	Auf dem ViPNet Coordinator HW/VA installieren Sie die ViPNet Schlüsseldistribution.	Installation der Schlüsseldistribution (auf S. 37)
☐	Verbinden Sie ViPNet Coordinator HW/VA-Knoten zum Ethernet-Netzwerk.	
☐	Stellen Sie das Datum und die Uhrzeit auf ViPNet Coordinator HW/VA ein.	Datum und Uhrzeit einstellen (auf S. 53)
☐	Vergewissern Sie sich, dass das ViPNet Coordinator HW/VA richtig funktioniert, indem Sie die Verbindung zwischen geschützten oder getunnelten Netzwerkknoten überprüfen.	Systeminformationen anzeigen (auf S. 58)

Achtung! Wenn Sie planen, ein Failover-Cluster (s. Zweckbestimmung des Failover-Systems auf S. 128) zu installieren, dann sollten Sie unbedingt die Anleitung im Dokument „ViPNet Coordinator HW/VA. Failover-Cluster“, Kapitel „Bereitstellung und Upgrade eines Failover-Clusters“ beachten.

Upgrade der Software auf ViPNet Coordinator HW/VA

Sobald eine neue Version von ViPNet Coordinator HW/VA veröffentlicht wird, empfehlen wir Ihnen, die Software auf dem Knoten zu aktualisieren. Das Upgrade gewährleistet die Stabilität der Software und ermöglicht den Einsatz neuer Funktionen. Zum Aktualisieren werden Upgradedateien benötigt, die ein Bestandteil des Software-Verteilungspakets sind oder direkt von einem Vertreter des InfoTeCS bezogen werden können (s. Kontakt auf S. 19).

Achtung! Wenn Sie auf eine ältere Version zurücksetzen möchten, dann installieren Sie die Upgrade-Paketdatei der entsprechenden Version. Das Zurücksetzen auf die Version 3.1 oder älter ist jedoch nicht möglich.

Es gibt mehrere Wege, das Appliance ViPNet Coordinator HW/VA zu aktualisieren:

- Remote-Upgrade mit Hilfe von ViPNet Network Manager. Das Upgrade von ViPNet Coordinator HW/VA kann auf mehreren Knoten gleichzeitig zentralisiert durchgeführt werden, ohne dass die Upgradedateien an die Netzwerkknotenbenutzer weitergeleitet werden. Das Remote-Upgrade stellt die einfachste Art dar, die Software eines Failover-Clusters (s. Zweckbestimmung des Failover-Systems auf S. 128) zu aktualisieren, da alle erforderlichen Schritte automatisch durchgeführt werden.

- Lokales Upgrade mit Hilfe eines USB-Datenträgers. Sie können das Upgrade manuell durchführen, wenn ViPNet Coordinator HW/VA offline ist und keine Dateien von ViPNet Network Manager empfangen kann. Dazu werden Upgradedateien benötigt, die Sie von einem Vertreter von InfoTeCS (s. Kontakt auf S. 19) beziehen können.

  - Das lokale Upgrade kann automatisch durchgeführt werden, ohne dass weitere Konfigurationsschritte notwendig sind. Kopieren Sie zum Durchführen des automatischen Upgrades die Upgrade-Paketdatei und die Upgrade-Konfigurationsdatei `hwinit-x.x-xxx_upgrade.xml` in den Stammordner eines USB-Datenträgers. Stellen Sie sicher, dass diese zwei Dateien die einzigen Dateien dieses Typs im Stammordner des USB-Datenträgers sind.

  - Das lokale Upgrade kann auch manuell unter Verwendung eines interaktiven Assistenten durchgeführt werden. Dies kann dann nützlich sein, wenn das Software-Upgradepaket nicht im Stammordner des USB-Laufwerks gespeichert werden soll.

Remote-Upgrade

Verwenden Sie das Programm ViPNet Network Manager, um die Software ViPNet Coordinator HW/VA sowohl auf einem gesonderten ViPNet Coordinator HW/VA-Knoten als auch in einem Failover-Cluster remote zu aktualisieren (s. Zweckbestimmung des Failover-Systems auf S. 128).

Gehen Sie wie folgt vor, um die Software remote zu aktualisieren:

1 Fordern Sie die Upgrade-Paketdatei für die Software beim Anbieter an.

2 Klicken Sie auf dem Knoten, auf dem die Software ViPNet Network Manager installiert ist, im Hauptmenü von ViPNet Network Manager auf **Extras** > **ViPNet Software Update**.

3 Folgen Sie den Anweisungen des **ViPNet Software Update** Assistenten.

Weitere Informationen zum Remote-Upgrade der Software s. Dokument „ViPNet VPN. Benutzerhandbuch“.

Automatisches lokales Upgrade

Gehen Sie wie folgt vor, um die Software auf ViPNet Coordinator HW/VA automatisch zu aktualisieren:

1 Kopieren Sie die Upgrade-Paketdatei `coordinator_driv_x.x-xxx.lzh` und die Upgrade-Konfigurationsdatei `hwinit-x.x-xxx_upgrade.xml` in den Stammordner eines USB-Datenträgers. Die Upgrade-Konfigurationsdatei ist ein Bestandteil des Software-Lieferumfangs (s. Lieferumfang auf S. 16).

2 Wenn das ViPNet Coordinator HW/VA-Appliance abgeschaltet ist, dann schalten Sie es ein.

3 Schließen Sie den USB-Datenträger an das Appliance an.

4 Starten Sie den Computer durch Ausführen des Befehls `machine reboot` neu.

   Nach dem Neustart erkennt die Software ViPNet Coordinator HW/VA automatisch die Upgradedateien auf dem USB-Datenträger. Das Software-Upgrade wird automatisch installiert.

5 Sobald der Installationsvorgang abgeschlossen ist, werden Sie aufgefordert, den USB-Datenträger wieder zu trennen. Entfernen Sie den USB-Datenträger und drücken Sie die **Eingabe**-Taste.

   Das Upgrade wird nach einem Neustart des Appliance fertiggestellt.

Manuelles lokales Upgrade

Achtung! Wenn Sie das Upgrade der Software eines Failover-Clusters manuell durchführen möchten, dann sollten Sie dazu unbedingt der Anleitung im Dokument „ViPNet Coordinator HW/VA. Failover-System“, Kapitel „Bereitstellung und Upgrade eines Failover-Clusters“ folgen.

Gehen Sie wie folgt vor, um die Software ViPNet Coordinator HW/VA manuell zu aktualisieren:

1. Kopieren Sie die Upgrade-Paketdatei `coordinator_driv_x.x-xxx.lzh` auf einen USB-Datenträger (das Kopieren in den Stammordner ist nicht erforderlich).
2. Wenn das ViPNet Coordinator HW/VA-Appliance abgeschaltet ist, dann schalten Sie es ein.
3. Melden Sie sich durch Ausführen des Befehls `enable` als Administrator an.
4. Führen Sie zum Starten des Upgradevorgangs den Befehl `admin upgrade software usb` aus.

   Sie werden aufgefordert, einen USB-Datenträger anzuschließen.
5. Schließen Sie den USB-Datenträger an das Appliance an und drücken die **Eingabe**-Taste.

   Der USB-Datenträger wird nach verfügbaren Upgrade-Paketdateien durchsucht. Es wird eine nummerierte Liste der Dateien angeblendet.
6. Geben Sie die Dateinummer ein und drücken die **Eingabe**-Taste.

   Warten Sie, bis der Upgradevorgang abgeschlossen ist. Dieser Vorgang kann einige Minuten in Anspruch nehmen. Sobald der Upgradevorgang abgeschlossen ist, wird die Befehlszeilenschnittstelle wieder verfügbar.
7. Starten Sie das Appliance durch Ausführen des Befehls `machine reboot` neu.

   Das Upgrade wird nach dem Neustart fertiggestellt.

ViPNet Coordinator HW/VA im ViPNet Network Manager einstellen

Das ViPNet Coordinator HW/VA-Appliance übernimmt im ViPNet Netzwerk die Rolle des Coordinators (s. Funktionen eines Coordinators im privaten ViPNet Netzwerk auf S. 25). Bevor ViPNet Coordinator HW/VA verwendet werden kann, sollte im Programm ViPNet Network Manager ein neuer Coordinator erstellt (oder ein bereits vorhandener Coordinator passend umkonfiguriert) werden und eine Schlüsseldistribution für diesen Coordinator generiert werden. Danach sollte diese Schlüsseldistribution auf dem ViPNet Coordinator HW/VA-Knoten installiert werden (s. Manuelle Schlüsselinstallation auf S. 38).

Hinweis. Weiter unten finden Sie die Anleitung für die Konfiguration der Knoten in ViPNet Network Manager der Version 4.1 oder höher. In früheren Versionen könnten einige der beschriebenen Einstellungen nicht verfügbar sein. In diesem Fall können Sie die betroffenen Einstellungen später über die Webschnittstelle oder unter Verwendung der Befehlszeile vornehmen (s. Verwalten von ViPNet Coordinator HW/VA-Knoten auf S. 46).

Gehen Sie im Hauptfenster von ViPNet Network Manager wie folgt vor, um einen ViPNet Coordinator HW/VA-Knoten zu erstellen und zu konfigurieren:

1 Klicken Sie in der Navigationsleiste mit der rechten Maustaste auf **Eigenes Netzwerk** und wählen Sie im Kontextmenü **Coordinator HW / VA hinzufügen**. Geben Sie einen Namen für den neuen Coordinator ein.

Hinweis. Die Eintrag **Coordinator HW / VA hinzufügen** wird dann verfügbar, wenn die Verwendung vpn ViPNet Coordinator HW/VA von Ihrer Lizenz für das ViPNet VPN-Netzwerk erlaubt ist. Anderenfalls wenden Sie an einen Vertreter der InfoTeCS GmbH.

2 Bei Bedarf fügen Sie Clients zu dem Coordinator hinzu.

3 Wählen Sie den neuen Coordinator in der Navigationsleiste aus.

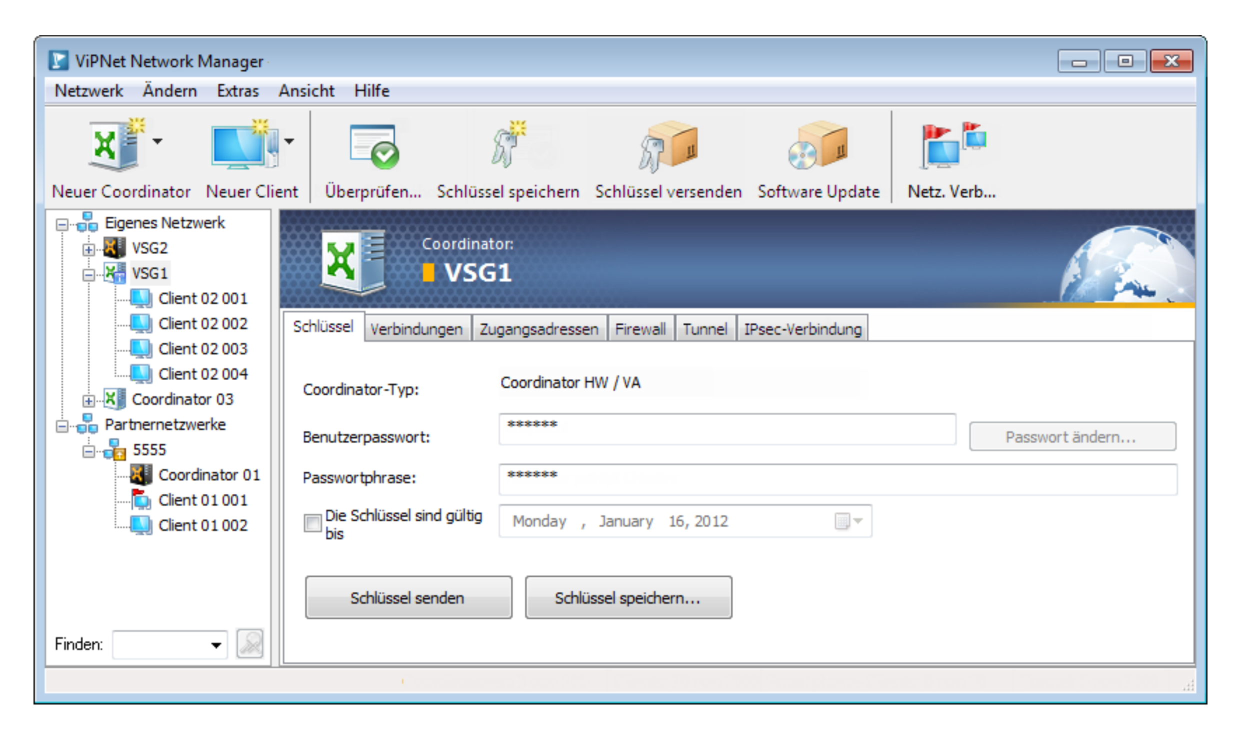


Abbildung 1: ViPNet Coordinator HW/VA im Programm ViPNet Network Manager einstellen

4 Wenn ein eigenes Benutzerpasswort von ViPNet Coordinator HW/VA angelegt werden soll, dann klicken Sie auf die Schaltfläche **Passwort ändern**. Wählen Sie im Fenster **Benutzerpasswort** die Option **Benutzerdefiniert**. Geben Sie das neue Passwort ein und bestätigen Sie es. Klicken Sie dann auf **OK**.

5 Konfigurieren Sie in der Registerkarte **Netzwerkeinstellungen** die Parameter der Netzwerkadapter:

- Konfigurieren Sie die Ethernet-Adapter (insbesondere die Methode der Zuweisung von IP-Adressen).
- Konfigurieren Sie die Wi-Fi-Adapter.

Hinweis. Wenn die ViPNet Netzwerkknotenschlüssel für ein Failover-Cluster (s. Failover-System auf S. 127) im Programm ViPNet Network Manager erstellt werden, dann sind keine zusätzlichen Einstellungen auf der Registerkarte **Netzwerkeinstellungen** nötig. Wenn Sie dort Änderungen vornehmen, werden diese vom Cluster ignoriert. Die Adapter werden in einem Cluster lokal konfiguriert (s. Dokument „ViPNet Coordinator HW/VA. Failover-System. Administratorhandbuch“.

---

6 Wenn Sie neue VPN-Clients an dem Coordinator hinzufügen möchten, dann geben Sie in der Registerkarte **Zugangsadressen** die IP-Adressen oder DNS-Namen an, die zum Zugang anderer Knoten zu dem Coordinator benutzt werden:

- Soll der Coordinator über statische IP-Adressen verfügen, geben Sie die IP-Adressen des Coordinators in der Liste **IP-Adressen** an.
- Soll der Coordinator über dynamische IP-Adressen verfügen, geben Sie in der Liste **DNS-Namen** die DNS-Namen des Coordinators an. Diese Namen müssen im DNS-Service registriert sein, z.B. DynDNS.

Tipp. Wenn Sie die IP-Adressen des Coordinators noch nicht wissen, können Sie ihnen später angeben, wenn Sie mit der Einrichtung von Coordinator fertig sind.

Wenn der Coordinator ausschließlich für Tunnelung verwendet werden soll, dann müssen keine Zugangsadressen festgelegt werden.

Hinweis. Das Hinzufügen von VPN-Clients wird von ViPNet Coordinator HW der Modifikationen HW 100 X1/X4/X5/X6 nicht unterstützt.

---

7 Geben Sie in der Registerkarte **Firewall** die Parameter für die Verbindung des Coordinators zu einem externen Netzwerk (z.B. zum Internet) an:

- Wenn der Coordinator direkt mit dem externen Netzwerk verbunden wird, deaktivieren Sie das Kontrollkästchen **Firewall verwenden**.
- Wenn die Verbindung des Coordinators zu einem externen Netzwerk über eine Firewall erfolgt, aktivieren Sie das Kontrollkästchen **Firewall verwenden**, in der Liste **Firewall-Typ** wählen Sie den richtigen Punkt und geben Sie die anderen Verbindungsparameter an.

8 Soll der Coordinator den Datenverkehr von offenen Netzwerkknoten tunneln, fügen Sie in der Registerkarte **Tunnel** in der Liste **IP-Adressen der getunnelten Verbindungen** die IP-Adressen von offenen Netzwerkknoten, die getunnelt werden sollen, hinzu.

9 Wenn Sie den ViPNet Coordinator HW/VA-Knoten als IPsec-Gateway verwenden möchten, konfigurieren Sie die erforderlichen Einstellungen auf der Registerkarte **IPsec-Verbindung**. Weitere Informationen s. Abschnitt Konfiguration des IPsec-Gateways (auf S. 103).

Achtung! Wenn Sie die Schlüsseldistribution automatisch auf den ViPNet Coordinator HW/VA-Knoten installieren möchten (s. Automatische Installation der Schlüsseldistribution auf S. 38), dann sollten Sie die IPsec-Verbindungseinstellungen erst nach erfolgter Installation der Schlüsseldistribution konfigurieren. Konfigurieren Sie nach der Installation der Schlüsseldistribution die IPsec-Verbindung im ViPNet Network Manager und versenden Sie die Schlüssel anschließend an ViPNet Coordinator HW/VA. Nach der Übernahme der Schlüssel auf dem Knoten treten die neuen Einstellungen in Kraft.

10 Sobald alle notwendigen Einstellungen vorgenommen wurden, klicken Sie in der Registerkarte **Schlüssel** auf **Schlüssel speichern** und geben den Ordner zum Speichern der Schlüsseldistributionen an.

Im angegebenen Ordner wird der Ordner `ViPNet_NNNN_keys` erstellt, wobei `NNNN` die Nummer Ihres ViPNet Netzwerks repräsentiert. Innerhalb des Ordners befinden sich folgende Elemente:

- Ein Unterordner, der die Schlüsseldistribution für den <Crtf_Product_name>-Knoten (Datei *.dst) und die Datei `hwinit_set.xml` enthält, die für die automatische Schlüsselinstallation verwendet wird (s. Automatische Installation der Schlüsseldistribution auf S. 38).
- Die Textdatei `ViPNet.txt`, in der die Benutzerpasswörter für den Netzwerkknoten enthalten sind.

11 Installieren Sie die Schlüsseldistribution auf ViPNet Coordinator HW/VA-Appliance (s. Manuelle Schlüsselinstallation auf S. 38).

Hinweis. Wenn ein oder mehrere der oben aufgelisteten Parameter nicht definiert worden sind, sollten sie im ViPNet Network Manager später angegeben werden. In diesem Fall können die Netzwerkknoten, die mit diesem Coordinator verbunden sind, bei der Schlüsselaktualisierung die IP-Adressen des Coordinators und aller von ihm getunnelten Knoten, sowie andere Parameter aus dem Programm ViPNet Network Manager ablesen.

12 Leiten Sie die Passwörter an die Knotenbenutzer weiter.

Detaillierte Informationen über die Einstellung von Netzwerkknoten-Parameter im ViPNet Network Manager Programm finden Sie im „ViPNet VPN. Benutzerhandbuch".

Installation der Schlüsseldistribution

Ein ViPNet Coordinator HW/VA-Knoten ist betriebsbereit, sobald Sie auf diesem Knoten eine Schlüsseldistribution installiert haben. Konfigurieren Sie dazu den ViPNet Coordinator HW/VA-Knoten im Programm ViPNet Network Manager, speichern Sie die Schlüssel des Knotens ab (s. ViPNet Coordinator HW/VA im ViPNet Network Manager einstellen auf S. 33) und übertragen Sie diese anschließend auf einem USB-Datenträger oder auf einer CD/DVD auf den zugehörigen Knoten. Es gibt zwei Wege, wie Sie eine Schlüsseldistribution auf einen ViPNet Coordinator HW/VA-Knoten installieren können:

- Die Schlüssel können von einem USB-Datenträger automatisch installiert werden. Die automatische Installation ist einfach und vor allem dann empfehlenswert, wenn der gegebene Knoten über keinen Bildschirm und keine Tastatur verfügt. Während der automatischen Installation müssen keine Einstellungen auf dem Knoten vorgenommen werden.

  Wenn Sie eine automatische Installation durchführen möchten, kopieren Sie die Schlüsseldistribution und die Konfigurationsdatei `hwinit_set.xml` (s. ViPNet Coordinator HW/VA im ViPNet Network Manager einstellen auf S. 33) vom ViPNet Network Manager knoten in den Stammordner des USB-Datenträgers. Stellen Sie vor der Installation der Schlüssel sicher, dass es neben der benötigten Schlüsseldistribution keine weiteren Schlüssel im Stammordner des USB-Datenträgers gibt.

- Die Schlüssel können manuell unter Verwendung eines USB-Datenträgers oder einer CD/DVD installiert werden. Es steht Ihnen dabei ein interaktiver Installationsassistent zur Verfügung. Bei der manuellen Installation können sich mehrere Schlüsseldistributionen auf dem Datenträger befinden. Die Schlüssel dürfen sowohl im Stammordner als auch in gesonderten Ordnern gespeichert sein. Diese Möglichkeit kann dann von Nutzen sein, wenn Sie vorhaben, mehrere Schlüsseldistributionen auf einen einzigen Datenträger zu kopieren, um sie später auf einige Knoten zu installieren. Während der manuellen Installation können Sie genau festlegen, welche Schlüsseldistribution auf welchen Knoten installiert wird.

  Wenn Sie eine manuelle Installation durchführen möchten, kopieren Sie die benötigten Schlüsseldistributionen auf den Datenträger. Es ist aber nicht nötig, die Konfigurationsdatei `hwinit_set.xml` auf den Datenträger zu kopieren.

Achtung! Wenn Sie möchten, ein Failover-Cluster (s. Zweckbestimmung des Failover-Systems auf S. 128) zu installieren, dann sollten Sie unbedingt die Anleitung im Dokument „ViPNet Coordinator HW/VA. Failover-Cluster“, Kapitel „Bereitstellung und Upgrade eines Failover-Clusters“ beachten.

Automatische Installation der Schlüsseldistribution

Zum automatischen Installieren der Schlüsseldistribution:

1. Schließen Sie den USB-Datenträger, der Konfigurationsdatei enthält (s. Installation der Schlüsseldistribution auf S. 37), an ViPNet Coordinator HW/VA-Knoten an.
2. Schalten Sie das Appliance ein. Die ViPNet Coordinator HW/VA-Software erkennt den USB-Datenträger mit der Schlüsseldistribution und leitet die automatische Schlüsselinstallation ein.

   Sobald der Installationsvorgang abgeschlossen ist, werden die ViPNet Coordinator HW/VA-Daemons automatisch gestartet.
3. Wenn nötig, konfigurieren Sie die Einstellungen von ViPNet Coordinator HW/VA (s. Kurzleitfaden auf S. 11).

Manuelle Schlüsselinstallation

Für die manuelle Installation der Schlüssel auf einen ViPNet Coordinator HW/VA-Knoten benötigen Sie einen USB-Datenträger oder eine CD/DVD mit den erforderlichen Schlüsseln (s. Installation der Schlüsseldistribution auf S. 37). Ein Assistent wird Sie durch die Installation führen. Dieser Assistent ermöglicht Ihnen außerdem die Konfiguration der wichtigsten Parameter von ViPNet Coordinator HW/VA. Zum Installieren der Schlüsseldistribution:

1. Fahren Sie das Appliance hoch und warten bis die gesamte Software geladen ist.
2. Sobald Sie nach dem Benutzernamen gefragt werden, tippen Sie `user` ein und drücken die Taste **Eingabe**.
3. Sobald Sie nach dem Passwort gefragt werden, tippen Sie ebenso `user` ein und drücken die Taste **Eingabe**.

   Nach einer erfolgreichen Anmeldung wird das Setupprogramm von ViPNet Coordinator HW/VA gestartet. Wählen Sie einen der zwei Modi des Setupprogramms:

   - 1 öffnet die Befehlszeilenschnittstelle. In diesem Fall können Sie die Einstellungen mit Hilfe der Tastatur eingeben.
   - 2 öffnet die grafische Oberfläche. In diesem Fall können Sie die Einstellugen durch Auswählen der entsprechenden Optionen mit Hilfe der Tastatur ausführen.

   Beide Modi sehen die gleiche Anzahl an Schritten für die Vorkonfiguration von ViPNet Coordinator HW/VA vor. Weiter unten in diesem Abschnitt beschreiben wir die

erforderlichen Aktionen für die Befehlszeilenschnittstellemodus. Wenn Sie den interaktiven Assistent benutzen, führen Sie gleichartige Schritte durch.

4 Wählen Sie für das Setupprogramm den Betriebsmodus Befehlszeilenschnittstelle, indem Sie „`1`“ eingeben und die **Eingabe**-Taste drücken.

5 Sobald Ihnen die Schlüsselinstallation angeboten wird („`Would you like to start installing keys or restoring configuration?`“), geben Sie das Zeichen „`y`“ ein und drücken **Eingabe**.

6 Wählen Sie den Installationsmodus für die Schlüsseldistribution („`Would you like installing keys from TFTP, USB or CD storage device?`“):

   - Wenn von einem USB-Datenträger installiert werden soll, geben Sie „`u`” ein und drücken Sie **Eingabe**.
   - Wenn von einer CD installiert werden soll, geben Sie „`c`” ein drücken Sie **Eingabe**.

7 Sobald Ihnen angeboten wird, ein USB-Speichermedium mit der Schlüsseldistribution an Ihrem ViPNet Coordinator HW/VA anzuschließen („`Insert USB storage device (or CD disk) with DST or VBE file and press Enter`“), schließen Sie den Datenträger mit der Schlüsseldistribution an und drücken **Eingabe**.

8 Sollte es auf dem Datenträger mehrere Schlüsseldistributionen geben, wird die Liste aller zur Verfügung stehenden Distributionen auf dem Bildschirm angezeigt. Wählen Sie bitte die richtige Distribution („`Choose file by number or press Enter for next page`“), indem Sie die Nummer der dem ViPNet Coordinator HW/VA entsprechenden Distribution angeben, und drücken **Eingabe**.

9 Bei der Anfrage nach dem Benutzerpasswort für den Netzwerkknoten geben Sie das Benutzerpasswort des Coordinators ein (s. ViPNet Coordinator HW/VA im ViPNet Network Manager einstellen auf S. 33) und drücken **Eingabe**. Wurde das Password erfolgreich angenommen, erscheint auf dem Bildschirm eine entsprechende Meldung.

10 Definieren Sie die Parameter für jeden der Coordinator-Netzwerkadapter:

   - Wenn Sie gefragt werden, ob ein Netzwerkadapter aktiviert werden soll („`Activate interface ethN?`“), dann geben Sie eines der folgenden Zeichen ein:
     - „`y`“ zum Aktivieren des Adapters;
     - „`n`“ zum Deaktivieren des Adapters;
     - „`x`“ zum Übernehmen der Adapterkonfiguration, die für diesen Adapter im Programm ViPNet Network Manager definiert wurde (Registerkarte **Netzwerkoptionen**) (s. ViPNet Coordinator HW/VA im ViPNet Network Manager einstellen auf S. 33). Diese Option ist nur dann verfügbar, wenn vom ViPNet Netzwerkadministrator zumindest eine Konfiguration für diesen Adapter in ViPNet Network Manager durchgeführt wurde.

Drücken Sie die **Eingabe**-Taste.

- Wenn Sie die Aktivierung des Adapters (Option „`y`“) veranlasst haben, dann werden Sie nun aufgefordert, die Verwendung eines DHCP-Servers für die Zuweisung der Netzwerkparameter an den Adapter zuzulassen („`Use dhcp on the interface ethN?`“). Geben Sie „`y`“ ein, um die dynamische Zuweisung der Parameter vom Server durchführen zu lassen, oder tippen Sie „`n`“ ein, um die statischen Einstellungen später zu konfigurieren. Drücken Sie dann die **Eingabe**-Taste.

Hinweis. Wenn Sie beschlossen haben, die Netzwerkparameter für alle Adapter zu einem späteren Zeitpunkt zu konfigurieren, dann werden Sie aufgefordert, die Adressen der DNS- und NTP-Server optional in einem der folgenden Schritte festzulegen (dies geschieht beim Einstellen der Systemzeit der Appliance).

---

11 Legen Sie die Zeitzone und die Systemzeit des Appliance fest. Dafür bietet der Assistent Ihnen an, Ihren Standort zu definieren:

- Sobald Ihnen die Kontinente zur Auswahl stehen („`Please select a continent or ocean`“), geben Sie die Ihrem Kontinent entsprechende Nummer ein und drücken **Eingabe**.
- Sobald Ihnen die Länder zur Auswahl stehen („`Please select a country`“), geben Sie die Ihrem Land entsprechende Nummer ein und drücken **Eingabe**.
- Sobald Ihnen die Zeitzonen zur Auswahl stehen („`Please select one of the following time zone regions`“), geben Sie die richtige Nummer ein und drücken **Eingabe**.
- Die dem angegebenen Standort entsprechende Zeitzone wird auf dem Bildschirm angezeigt. Um diese Zeitzone zu übernehmen, geben Sie „`1`“ („`Yes`“) ein. Um den Standort neu zu definieren, geben Sie „`2`“ („`No`“) ein. Drücken Sie **Eingabe**.
- Nachdem die Zeitzone angenommen wurde, wird die Systemzeit angezeigt.
  - Um die Systemzeit zu übernehmen, drücken Sie **Eingabe**.
  - Um die Zeit zu ändern, geben Sie Datum und Zeit an und drücken **Eingabe**. Bitte halten Sie sich an dieses Format: JJJJ-MM-TT hh:mm:ss.

12 Nachdem die Konfiguration durchgeführt wurde, wird Ihnen angeboten, den ViPNet Coordinator HW/VA Kommandointerpreter zu starten („`Do you want to start the command shell now?`“). Um den Kommandointerpreter zu starten, geben Sie „`y`“ ein. Um auf den Start zu verzichten, geben Sie „`n`“ ein. Danach drücken Sie **Eingabe**.

13 Nach der Installation der Schlüsseldistribution stellen Sie den Coordinator ein (s. Konfiguration der Systemparameter auf S. 52).

Löschen der Schlüssel in ViPNet Coordinator HW/VA

Manchmal kommt es vor, dass die Schlüssel auf dem ViPNet Coordinator HW/VA gelöscht werden sollen. Beispiel: ein ViPNet Coordinator HW/VA wird als Coordinator im Netzwerk eingesetzt, soll aber als neuer Coordinator in einem anderen Netzwerk bereitgestellt werden. In diesem Fall muss eine neue Schlüsseldistribution auf diesen Coordinator installiert werden. Zuvor müssen die vorhandenen Schlüssel gelöscht werden. Dazu:

1. Melden Sie sich durch Ausführen des Befehls `enable` (s. Verwalten von ViPNet Coordinator HW/VA-Knoten auf S. 46) als Administrator an.
2. Führen Sie den Befehl `admin remove keys` aus.
3. Bestätigen Sie das Löschen der Schlüssel, indem Sie **Yes** eingeben und dann die **Eingabe**-Taste drücken.
4. Warten Sie, während die Schlüssel gelöscht werden. Anschließend können Sie eine neue Schlüsseldistribution installieren (s. Installation der Schlüsseldistribution auf S. 37).

Zurücksetzen der ViPNet Coordinator HW/VA-Parameter

Wenn Sie den ursprünglichen Herstellerzustand des ViPNet Coordinator HW/VA-Appliance wiederherstellen, dann werden alle benutzerdefinierten Einstellungen, Schlüssel und Logdateien verworfen. Die Software wird in den Status zurückgesetzt, in dem sie sich sofort nach der Installation befunden hat.

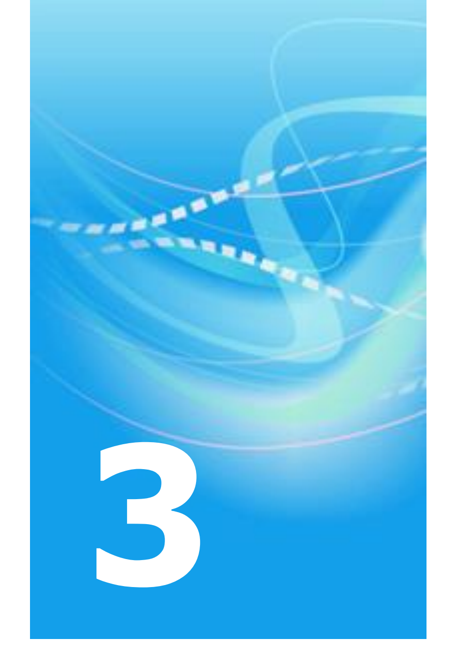
Das Zurücksetzen des Appliance ist möglicherweise in den folgenden Fällen nötig:

- Ein ViPNet Coordinator HW/VA-Knoten soll für andere Benutzer bereitgestellt werden. Die Schlüssel des Knotens, die Logdateien und andere Daten über den Status des Knotens sollen diesen Benutzern jedoch nicht zur Verfügung stehen.
- Wegen eines Softwarefehlers ist der Zugriff auf die Benutzeroberfläche nicht mehr möglich.

Benutzen Sie zum Wiederherstellen des Originalzustands einen USB-Wechseldatenträger, der die spezielle Konfigurationsdatei `hwinit_reset.xml` enthält. Diese Datei wird auf dem ViPNet Network Manager-Knoten im Ordner `ViPNet_NNNN_keys` (wobei `NNNN` die Nummer Ihres ViPNet Netzwerks repräsentiert) beim Speichern der Schlüssel für den ViPNet Coordinator HW/VA-Knoten automatisch erstellt (s. ViPNet Coordinator HW/VA im ViPNet Network Manager einstellen auf S. 33).

Zum Zurücksetzen der ViPNet Coordinator HW/VA-Parameter:

1. Speichern Sie in ViPNet Network Manager die Schlüssel für den ViPNet Coordinator HW/VA-Knoten. Die Datei `hwinit_reset.xml` wird automatisch erstellt.
2. Kopieren Sie die Datei `hwinit_reset.xml` aus dem Ordner `ViPNet_NNNN_keys` in den Stammordner eines USB-Wechseldatenträgers.
3. Wenn das ViPNet Coordinator HW/VA-Appliance eingeschaltet ist, schalten Sie es aus.
4. Schließen Sie den USB-Datenträger an das Appliance an.
5. Schalten Sie den Computer ein. Die ViPNet Coordinator HW/VA-Software erkennt den USB-Datenträger mit der Datei `hwinit_reset.xml`. Die ViPNet Schlüssel werden deinstalliert und die Software-Einstellungen werden automatisch zurückgesetzt. Der Computer wird heruntergefahren.



Zugreifen auf ViPNet Coordinator HW/VA

Zugriffsmodi und Berechtigungen

Die Bereitstellung und Wartung eines ViPNet Coordinator HW/VA-Knotens wird in einem der folgenden Zugriffsmodi durchgeführt:

- Modus „Keine Authentifizierung“;
- Modus „Knotenbenutzer“;
- Modus „Knotenadministrator“;
- Modus „Netzwerkadministrator“.

Für den Zugriff auf den Knoten ist eventuell die Authentifizierung durch ein Passwort erforderlich.

Tabelle 9. Verfügbare Aktionen abhängig vom Zugriffsmodus

	Zugriffsmodus			
	Keine Authentifizierung	**Knotenbenutzer**	**Knotenadministrator**	**Netzwerkadministrator**
Zugang				
Schnittstelle	USB-Laufwerk (localer Zugang)	Webschnittstelle (Remotezugang), Befehlszeilenschnittstelle (localer Zugang/ Remotezugang)		Programm ViPNet Network Manager (Remotezugang)
Authentifizierung	nein	Benutzer passwort	Benitzerpasswort, Passwort des ViPNet Knotenadministrators	ViPNet Network Manager Benutzerpasswort
Setup				
Installation der ViPNet Software	**ja**	**ja**	**ja**	nein
Installation der Schlüssel	**ja**	**ja**	**ja**	nein
Upgrade der ViPNet Software	**ja**	**ja**	**ja**	**ja**
Wartung				

Überwachung und Diagnose	nein	**ja**	**ja**	nein
Konfiguration der Systemeinstellungen	nein	nein	**ja**	nein
Konfiguration der Netzwerkadapter	nein	nein	**ja**	**ja**
Konfiguration der integrierten Firewall	nein	nein	**ja**	nein
Starten und Anhalten der integrierten Dienste	nein	**ja**	**ja**	nein
Konfiguration der integrierten Dienste	nein	nein	**ja**	nein
Konfiguration des ViPNet und IPsec VPN	nein	nein	**ja**	**ja**

Weitere Informationen zum Abrufen der Knotenbenutzer- und Knotenadministratorpasswörter s. Dokument „ViPNet VPN. Benutzerhandbuch“, Kapitel „Verwaltung eines ViPNet Netzwerks“.

Verwalten von ViPNet Coordinator HW/VA-Knoten

Das Verwalten von ViPNet Coordinator HW/VA kann auf einem der folgenden Wege erfolgen:

- Lokal unter Verwendung eines USB-Laufwerks, um eine Schlüsseldistribution zu installieren (s. Installation der Schlüsseldistribution auf S. 37) oder ein Upgrade von ViPNet Coordinator HW/VA (s. Upgrade der Software auf ViPNet Coordinator HW/VA auf S. 30) ohne Benutzeranmeldung durchzuführen.
- Aus dem ViPNet Network Manager: so können die Netzwerkeinstellungen und externen Firewalloptionen von ViPNet Netzwerkadministratoren konfiguriert werden. Diese Einstellungen werden dann auf dem ViPNet Coordinator HW/VA-Knoten angewendet, wenn dort eine Schlüsseldistribution installiert wird (s. Installation der Schlüsseldistribution auf S. 37) oder Netzwerkknotenschlüssel empfangen werden, die vom ViPNet Network Manager über das ViPNet Netzwerk versendet wurden.

  Obwohl Sie diese Parameter auch auf eine andere Weise konfigurieren können, empfehlen wir ausdrücklich, die Parameter der externen Firewall und die Adressen der getunnelten Knoten in ViPNet Network Manager einzustellen. Es wird außerdem empfohlen, die IP-Adressen und DNS-Namen in ViPNet Network Manager zu definieren. Die Änderungen in den Einstellungen anderer Knoten werden dann über den Versand von Schlüsselupdates zentralisiert durchgeführt, wodurch die Netzwerkadministration vereinfacht wird.

  Weitere Informationen über die Arbeit mit ViPNet Network Manager s. Dokument „ViPNet VPN. Benutzerhandbuch."

  Hinweis. Wenn Sie das Programm ViPNet Network Manager der Version 4.0 oder älter verwenden, dann haben Sie keinen Zugriff auf die Netzwerkeinstellungen des ViPNet Coordinator HW/VA-Knotens.

- Über die Webschnittstelle: so können die Netzwerkeinstellungen, die Systemparameter und die integrierten Dienste des Knotens konfiguriert werden. Die Webschnittstelle wird auf einem Webserver, der in dem ViPNet Coordinator HW/VA-Appliance integriert ist, zur Verfügung gestellt.

  Mit Hilfe der Webschnittstelle kann das ViPNet Coordinator HW/VA von einem beliebigen ViPNet Knoten, der mit dem ViPNet Coordinator HW/VA innerhalb des ViPNet Netzwerks verbunden ist, bequem konfiguriert werden. Zusätzlich kann das

ViPNet Coordinator HW/VA von einem Computer konfiguriert werden, der sich im gleichen lokalen Netzwerk befindet. Geben Sie in der Adresszeile eines Webbrowsers die IP-Adresse des ViPNet Coordinator HW/VA-Knotens ein (s. Anmeldung an der Webschnittstelle auf S. 48), um auf die Webschnittstelle zuzugreifen. Benutzen Sie zum Anmelden das Passwort des ViPNet Netzwerkknotenbenutzers.

- Über die Befehlszeilenschnittstelle: so können alle Knotenparameter konfiguriert werden. Einige Einstellungen können ausschließlich unter Verwendung der Befehlszeile konfiguriert werden (z. B. die Parameter der integrierten Firewall).

  So können Sie auf Befehlszeilenschnittstelle zugreifen:

  - local, indem Sie ein Monitor und Tastatur an dem Appliance schließen,
  - remote über das SSH-Protokoll.

  Die Befehlszeile wird bei der Anmeldung eines Benutzers in ViPNet Coordinator HW/VA automatisch gestartet. Verwenden Sie zur Anmeldung in ViPNet Coordinator HW/VA das Logon `user` und Ihr Benutzerpasswort.

  Der Kommandointerpreter kann in einem der zwei folgenden Zugriffsmodi (s. Zugriffsmodi und Berechtigungen auf S. 44) ausgeführt werden:

  - Benutzermodus (standardmäßig eingestellt), in welchem ein eingeschränkter Satz an Befehlen zur Verfügung steht. Als Eingabeaufforderung der Kommandozeile wird in diesem Modus das Symbol ‚>' verwendet.
  - Netzwerkknoten-Administratormodus, der den Zugang zu allen verfügbaren Befehlen ermöglicht. Als Eingabeaufforderung der Kommandozeile wird das Symbol ‚#' verwendet. Zum Wechseln in den Administratormodus sollten der Befehl `enable` ausgeführt und das Administratorpasswort des Netzwerkknotens eingegeben werden. Zum Beenden des Administratormodus sollte der Befehl `exit` ausgeführt werden.

  Die in den Befehlsbeschreibungen verwendete Notation wird im Abschnitt Verwendete Konventionen (auf S. 9) behandelt. Für detallierte Beschreibung der Befehle von ViPNet Coordinator HW/VA s. „ViPNet Coordinator HW/VA. Referenzhandbuch".

Hinweis. Sie können auf einen ViPNet Coordinator HW/VA-Knoten von anderen ViPNet Knoten über die Web- oder Befehlszeilenschnittstelle ohne irgendwelche zusätzlichen Einstellungen zugreifen. Wenn Sie von einem Knoten zugreifen möchten, auf dem keine <Brand> Software installiert ist, dann sollten Sie zunächst die Filter auf dem ViPNet Coordinator HW/VA konfigurieren, um die eingehenden HTTP- oder SSH-Verbindungen vom entsprechenden Knoten zu erlauben (s. Regeln zur Filterung des Traffics auf S. 112).

Anmeldung an der Webschnittstelle

Die Webschnittstelle von ViPNet Coordinator HW/VA stellt eine einfache Möglichkeit dar, Netzwerkverbindungen, Systemeinstellungen und integrierte Dienste eines ViPNet Coordinator HW/VA-Knotens zu konfigurieren.

Nachdem ein ViPNet Coordinator HW/VA bereitgestellt wurde, einschließlich der Installation einer Schlüsseldistribution (s. Installation der Schlüsseldistribution auf S. 37), können Sie auf das gegebene ViPNet Coordinator HW/VA über seine Webschnittstelle zugreifen. Führen Sie dazu auf einem geschützten Netzwerkknoten, der mit dem gegebenen ViPNet Coordinator HW/VA verbunden ist, einen der folgenden Schritte aus:

- Im Programm ViPNet Monitor:
  - Öffnen Sie den Bereich **Privates Netzwerk**.
  - Wählen Sie in der Panel-Ansicht den ViPNet Coordinator HW/VA-Knoten aus.
  - Klicken Sie in der Symbolleiste auf **Web** .

    Im Standardbrowser wird die Anmeldeseite geöffnet.
- Öffnen Sie die Anmeldeseite von ViPNet Coordinator HW/VA in Ihrem Webbrowser, indem Sie die entsprechende IP-Adresse in der Adresszeile eingeben.

Hinweis. Auf diese Weise können Sie von jedem Knoten, der sich im gleichen lokalen Netzwerk befindet, auf das ViPNet Coordinator HW/VA zugreifen. Voraussetzung dafür ist jedoch, dass die Filter von ViPNet Coordinator HW/VA eingehende HTTP-Verbindungen mit diesem Knoten erlauben (s. Regeln zur Filterung des Traffics auf S. 112).

Gehen Sie auf der Anmeldeseite wie folgt vor:

1. Geben Sie ein Benutzerpasswort des Netzwerkknotens im entsprechenden Feld ein.
2. Klicken Sie auf **Anmelden**. Die Startseite wird geöffnet.

   Nachdem Sie sich als Benutzer angemeldet haben, können Sie die Einstellungen von ViPNet Coordinator HW/VA durchsehen, jedoch keine Änderungen an diesen Einstellungen vornehmen.
3. Geben Sie Administratorpasswort ein, um die Einstellungen von ViPNet Coordinator HW/VA zu konfigurieren. Um als Administrator anzumelden:

   3.1 Klicken Sie auf **Als Administrator anmelden** in der rechten oberen Ecke der Webseite.

3.2 Geben Sie das Administratorpasswort im Fenster **Administrator-Login** ein.

Es können mehrere Benutzersitzungen parallel gestartet werden, es kann aber nur eine Administratorsitzung gleichzeitig am Laufen sein. Wenn sich ein anderer Administrator anmeldet, während Ihre Administratorsitzung aktiv ist, dann wird Ihre Sitzung unterbrochen.

Beachten Sie bitte, dass die Einstellungen von ViPNet Coordinator HW/VA während Ihrer Sitzung als Benutzer von einem Administrator in einer anderen Sitzung geändert werden können. In diesem Fall werden Sie die geänderten Einstellungen nicht sehen können, bis Sie die Webseite in Ihrem Webbrowser aktualisieren.

Hinweis. Drücken Sie die Taste **F5**, um die Daten auf der Weboberfläche von ViPNet Coordinator HW/VA zu aktualisieren.

4 Wenn Sie Ihre Arbeit mit der Webschnittstelle von ViPNet Coordinator HW/VA beenden möchten, klicken Sie auf **Abmelden** in der rechten oberen Ecke der Webseite. Beachten Sie bitte, dass Sie bei längerer Inaktivität automatisch abgemeldet werden.

Verwaltung von ViPNet Coordinator HW/VA über die Webschnittstelle

Über die Webschnittstelle haben Sie Zugriff auf die folgenden Parameter:

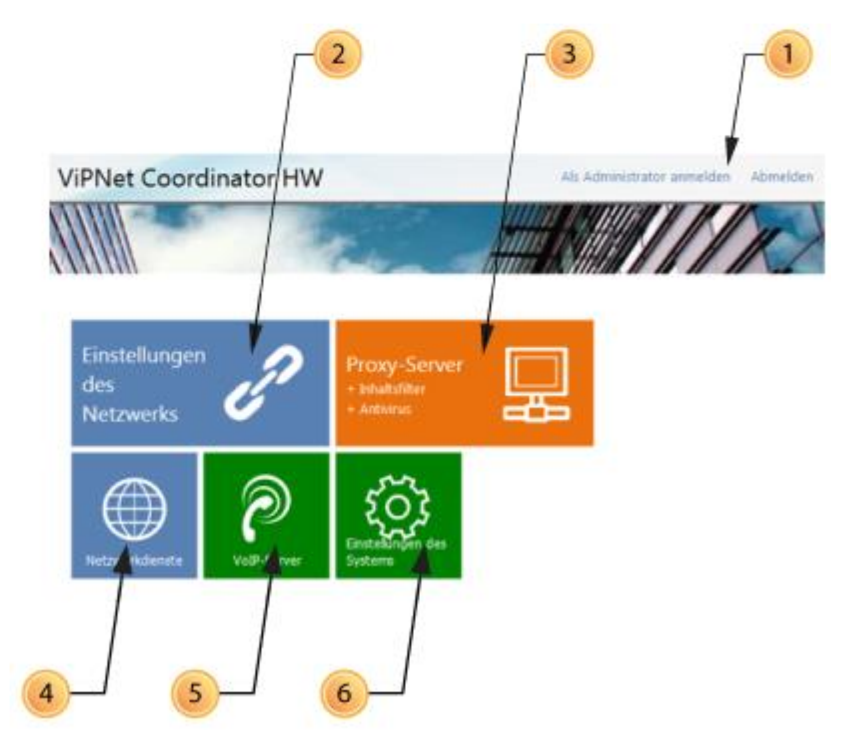


Abbildung 2: Startseite der Webschnittstelle

1 Authentisierungsmodus (s. Zugriffsmodi und Berechtigungen auf S. 44):

- Im Modus „Knotenbenutzer“ können Sie:
    - die Einstellungen des Knotens einsehen, jedoch nicht ändern.
    - integrierte Dienste aktivieren und deaktivieren und ihre Einstellungen einsehen
- Im Modus „Knotenadministrator“ können Sie die Einstellungen des Knotens einsehen und ändern.

2 Netzwerkeinstellungen (s. Konfiguration der Netzwerkeinstellungen von ViPNet Coordinator HW/VA mit Hilfe der Webschnittstelle auf S. 69):

- Verbinden zu einem Ethernet-Netzwerk.
- Verbinden zu einem Wi-Fi-Netzwerk.
- Bearbeiten der Routingtabelle.

3 Proxyserver-Komponenten (s. Konfiguration des Proxy-Servers auf S. 89):

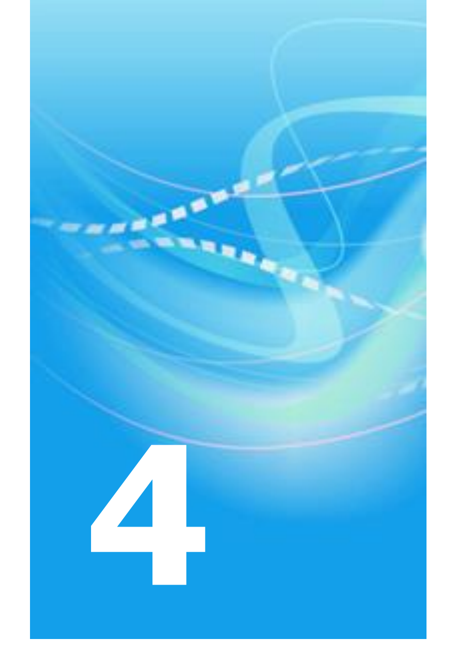
- Allgemeine Proxyserver-Einstellungen.
- Inhaltsfilter.
- Antivirus.

4 Netzwerkdienste:

- DHCP-Server (s. Parameter des NTP-Servers einstellen auf S. 86).
- NTP-Server (s. Parameter des NTP-Servers einstellen auf S. 86).
- DNS-Server (s. Parameter des DNS-Servers einstellen auf S. 85).

5 VoIP-Server (s. Konfiguration des VoIP-Servers auf S. 98).

6 Systemeinstellungen (s. Konfiguration der Systemparameter auf S. 52).



Konfiguration der Systemparameter

Datum und Uhrzeit einstellen

Damit ViPNet Coordinator HW/VA ordnungsgemäß mit anderen ViPNet Netzwerkknoten kommunizieren kann, sollten Sie das Systemdatum und die Systemzeit wie nachfolgend beschrieben konfigurieren.

Achtung! Wenn das Systemdatum und -uhrzeit nicht korrekt konfiguriert wurden, können verschlüsselte Verbindungen zu anderen ViPNet Netzwerkknoten blockiert werden.

Gehen Sie wie folgt vor, um das Systemdatum und die Systemzeit einzustellen:

1 Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).

2 Klicken Sie auf der Startseite auf **Einstellungen des Systems**.

3 Klicken Sie im oberen Fensterteil auf **Datum- und Uhrzeiteinstellungen**.

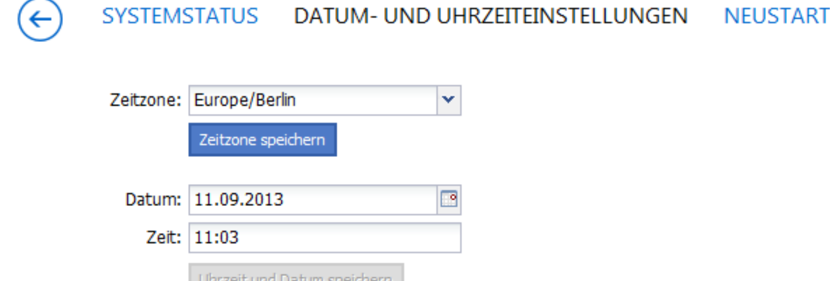


Abbildung 3: Ändern der Datum- und Uhrzeiteinstellungen

4 Zum Ändern der Zeitzone:

4.1 Wählen Sie in der Liste **Zeitzone** das geografische Gebiet aus, in dem sich der ViPNet Coordinator HW/VA-Knoten befindet.

4.2 Klicken Sie auf **Zeitzone speichern**. Die aktuelle Uhrzeit im Feld darunter wird automatisch geändert.

5 Zum Ändern des aktuellen Datums und der aktuellen Uhrzeit:

5.1 Klicken Sie auf das Symbol neben dem Feld **Datum** und geben mit Hilfe des Kalenders das aktuelle Datum an.

5.2 Geben Sie im Feld **Zeit** die aktuelle Uhrzeit im 24-Stunden-Format `HH:MM` ein.

5.3 Klicken Sie auf **Uhrzeit und Datum speichern**.

Konfiguration der Auslagerungsdatei

Die Auslagerungsdatei wird als zusätzlicher virtueller Speicher genutzt, um das zur Verfügung stehende Speichervolumen auf dem Appliance zu erweitern. Um Auslagerungsdatei zu konfigurieren, verwenden Sie den Kommandointerpreter (s. Kurzleitfaden auf S. 11).

Hinweis. Das Vergrößern des virtuellen Speichers durch Auslagerung wird von ViPNet Coordinator HW der Modifikationen HW 100 X1/X4/X5/X6 nicht unterstützt.

Führen Sie die folgenden Schritte aus, um die Parameter der Auslagerungsdatei zu konfigurieren:

- Benutzen Sie den folgenden Befehl, um die maximale Größe der Auslagerungsdatei festzulegen:

  ```
  machine swap set <Größe in MB>
  ```

  Wenn die festgelegte Größe der Auslagerungsdatei den zur Verfügung stehenden freien Speicherplatz auf dem Laufwerk übersteigt, wird eine entsprechende Meldung angezeigt.

  Achtung! Nachdem die Größe der Auslagerungsdatei festgelegt wurde, sollten auf dem Laufwerk noch mindestens 256 MB freier Speicherplatz verbleiben.

- Benutzen Sie den folgenden Befehl, um die Verwendung der Auslagerungsdatei zu aktivieren:

  ```
  machine swap mode on
  ```

- Führen Sie den folgenden Befehl aus, um Informationen über die Speicherverwendung und die Auslagerungsdatei anzuzeigen:

  ```
  machine show memory
  ```

- Benutzen Sie den folgenden Befehl, um die Verwendung der Auslagerungsdatei zu deaktivieren:

  ```
  machine swap mode off
  ```

  Nach Ausführung dieses Befehls wird die Auslagerungsdatei gelöscht.

Parameter für Systemprotokoll einstellen

Das Systemprotokoll enthält Daten über Ereignisse, die während der Laufzeit der Software ViPNet Coordinator HW/VA aufgetreten sind. Das Ereignisprotokoll kann auf dem lokalen Laufwerk oder auf einem beliebigen Knoten, der entsprechend konfiguriert wurde, gespeichert werden.

Hinweis. Sie können mit Hilfe der Webschnittstelle von ViPNet Coordinator HW/VA weder Logdatei-Einstellungen konfigurieren noch die Logdatei anzeigen. Verwenden Sie dazu den Kommandointerpreter (s. Kurzleitfaden auf S. 11).

Benutzen Sie die folgenden Befehle, um mit dem Ereignisprotokoll zu arbeiten:

- Führen Sie den folgenden Befehl aus, um den Knoten anzugeben, auf dem das Ereignisprotokoll gespeichert werden soll, oder um das Ereignisprotokoll zu deaktivieren:

  ```
  machine set loghost {local | <IP-Adresse> | null}
  ```

  Geben Sie einen der folgenden Werte an, um den Knoten zu definieren:

  - `local` – lokales Laufwerk von ViPNet Coordinator HW/VA,
  - `IP-Adresse` – IP-Adresse des Knotens, an welchen Daten über Systemereignisse gesendet werden sollen,

    Hinweis. Wenn es sich nicht um einen geschützten Knoten handelt, dann konfigurieren Sie eine Firewall-Regel (s. Regeln zur Filterung des Traffics auf S. 112), die den an diesen Knoten adressierten Traffic über UDP und Port 514 zulässt.

  - `null` – Ereignisprotokoll nicht speichern.

- Wenn das Ereignisprotokoll auf dem lokalen Laufwerk gespeichert wird, dann führen Sie den folgenden Befehl aus, um das Log anzuzeigen:

  ```
  machine show logs
  ```

- Ereignisprotokolle, die auf dem lokalen Laufwerk gespeichert werden, können auf einen USB-Wechseldatenträger mit Dateisystem FAT32 oder ext2 exportiert werden. Schließen

Sie dazu den USB-Datenträger an ViPNet Coordinator HW/VA an und führen Sie den folgenden Befehl aus:

```
admin export logs usb
```

- Führen Sie den folgenden Befehl aus, um das Ereignisprotokoll auf dem lokalen Laufwerk zu löschen:

```
admin remove logs
```

Systeminformationen anzeigen

Gehen Sie wie folgt vor, um Informationen über die Auslastung von CPU und Speicher zu erhalten und den Status der ViPNet Coordinator HW/VA-Komponenten anzuzeigen:

1 Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA (s. Anmeldung an der Webschnittstelle auf S. 48).

2 Klicken Sie auf der Startseite auf **Einstellungen des Systems**.

3 Klicken Sie im oberen Bereich der nächsten Seite auf **Systemstatus**.

Es werden der ViPNet Bezeichner des Knotens, der Status der Softwarekomponenten, die Speicherdaten sowie die Zeitdiagramme zur CPU- und Speicherauslastung angezeigt.

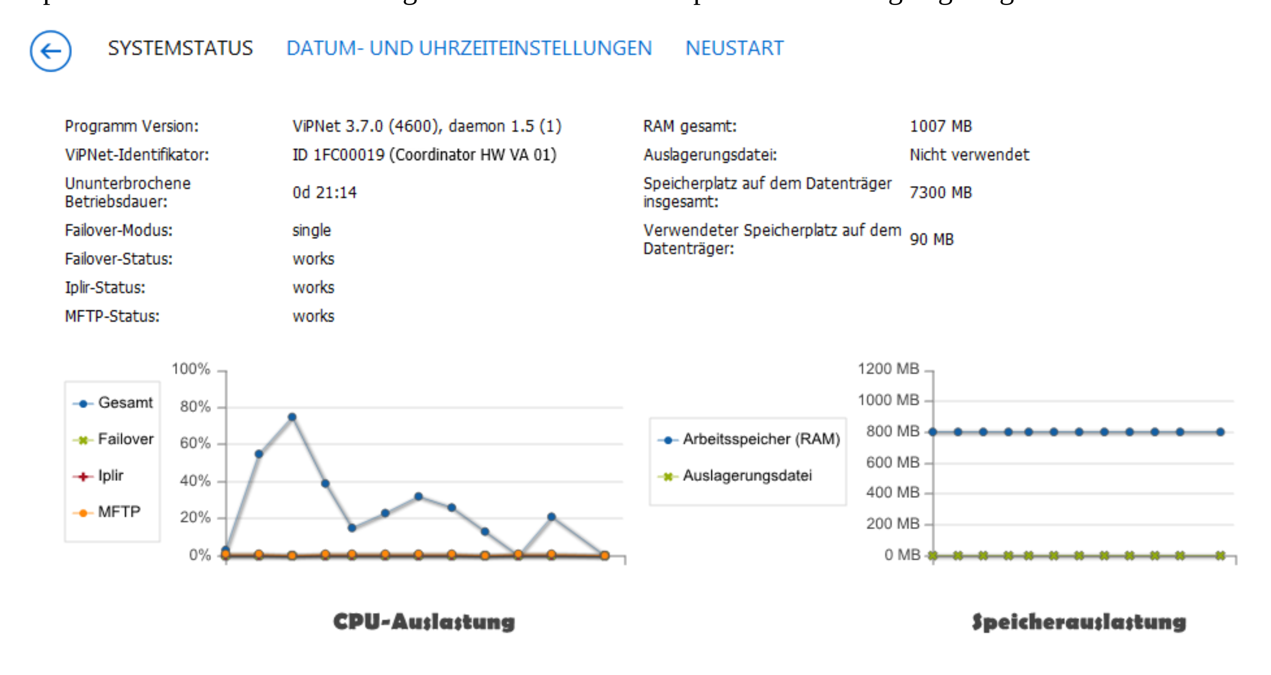


Abbildung 4: Anzeigen des Systemstatus

4 Wenn Sie detaillierte Informationen zu den Versionen von ViPNet Coordinator HW/VA-Komponenten anzeigen möchten, klicken Sie auf **Über ViPNet Coordinator HW/VA** im unteren Fensterteil.

Benutzen Sie die folgenden Befehle (s. Kurzleitfaden auf S. 11), um den Status und die unterschiedlichen Komponenten von ViPNet Coordinator HW/VA zu überprüfen und die Logdateien anzuzeigen:

- Zum Überprüfen der Verbindung zu einem offenen Knoten führen Sie den folgenden Befehl aus:

  ```
  inet ping <IP-Adresse>
  ```

- Zum Überprüfen der Verbindung zu einem geschützten ViPNet Knoten führen Sie den folgenden Befehl aus:

  ```
  iplir ping <ViPNet Netzwerkknoten-ID>
  ```

  Bei der Eingabe der ID stehen dem Benutzer die Features Autovervollständigung und Tipps zur Seite. Tipp-Daten werden aus der Verbindungsliste des ViPNet Coordinator HW/VA-Knotens bezogen.

- Zum Anzeigen der Konfigurationsdatei der Firewall (s. Konfiguration der integrierten Firewall auf S. 105) führen Sie den folgenden Befehl aus:

  ```
  iplir show config firewall
  ```

- Führen Sie zum Anzeigen der Logdatei registrierter IP-Pakete (s. Logdatei registrierter IP-Pakete anzeigen auf S. 117) den folgenden Befehl aus:

  ```
  iplir view
  ```

- Verwenden Sie zum Anzeigen des Systemprotokolls (s. Parameter für Systemprotokoll einstellen auf S. 56), der sich auf dem lokalen Laufwerk befindet, den Befehl:

  ```
  machine show logs
  ```

ViPNet Coordinator HW/VA zum Netzwerk verbinden

Über Konfiguration von Netzwerkeinstellungen

Sie können die Netzwerkeinstellungen von ViPNet Coordinator HW/VA auf eine der folgenden Arten konfigurieren:

- Remote von der Arbeitsstation des VPN-Administrators (s. Konfiguration der Netzwerkeinstellungen von ViPNet Coordinator HW/VA in ViPNet Network Manager auf S. 62).
- Remote von einem anderen ViPNet-Knoten, der mit ViPNet Coordinator HW/VA verbunden ist, über die Webschnittstelle (s. Konfiguration der Netzwerkeinstellungen von ViPNet Coordinator HW/VA mit Hilfe der Webschnittstelle auf S. 69).

  Dieser Ansatz ist nur dann möglich, wenn ViPNet Coordinator HW/VA im Netzwerk erreichbar ist.

- Mit Hilfe der Befehlszeile entweder lokal oder über das SSH-Protokoll (s. Aufbau der Verbindung zu einem Ethernet-Netzwerk unter Verwendung der Befehlszeilenschnittstelle auf S. 79). Dieser Ansatz ist in den folgenden Fälle empfohlen:
  - Wenn der Zugriff anderer Knoten auf den ViPNet Coordinator HW/VA-Knoten nicht mehr möglich ist.

    Nachdem der Zugang anderer Computer zum Knoten wiederhergestellt ist, können Sie den Rest der erforderlichen Netzwerkeinstellungen im ViPNet Network Manager oder über die Weboberfläche konfigurieren.

  - Wenn Sie Failover-Cluster (s. Zweckbestimmung des Failover-Systems auf S. 128) konfigurieren möchten.

Achtung! Die Befehlszeilenschnittstelle stellt die einzige korrekte Möglichkeit zur Konfiguration der Netzwerkadapter in einem Failover-Cluster dar. Alle Einstellungen, die Sie auf der Arbeitsstation des Administrators (in ViPNet Network Manager) oder über die Webschnittstelle vornehmen, werden im Cluster entweder nicht angewendet oder führen zu Konflikten in der Clusterkonfiguration.

Konfiguration der Netzwerkeinstellungen von ViPNet Coordinator HW/VA in ViPNet Network Manager

Achtung! Wenn Sie mit einem Failover-Cluster arbeiten, dann sollten Sie keine Netzwerkeinstellungen in ViPNet Network Manager konfigurieren, da die vorgenommenen Einstellungen entweder nicht angewendet werden oder zu Störungen in der Cluster-Konfiguration führen können. Verwenden Sie zum Konfigurieren der Netzwerkeinstellungen auf dem Cluster die Befehlszeilenschnittstelle (s. Aufbau der Verbindung zu einem Ethernet-Netzwerk unter Verwendung der Befehlszeilenschnittstelle auf S. 79).

Gehen Sie folgendermaßen vor, um die Netzwerkeinstellungen von ViPNet Coordinator HW/VA in ViPNet Network Manager zu konfigurieren:

1. Konfigurieren Sie die Verbindung zu einem Ethernet-Netzwerk (s. Verbinden zu einem Ethernet-Netzwerk mit Hilfe des ViPNet Network Manager auf S. 63).
2. Konfigurieren Sie bei Bedarf die Tunnelung (s. Konfiguration der Tunnelung auf einem ViPNet Coordinator HW/VA auf S. 67).
3. Versenden Sie Netzwerkknotenschlüssel an den Netzwerkknoten (s. Dokument „ViPNet VPN. Benutzerhandbuch”).
4. Führen Sie eine der folgenden Aktionen durch:
   - Wenn Sie das Setup von ViPNet Coordinator HW/VA durchführen und noch keine Schlüsseldistribution installiert haben:
     - Erstellen Sie eine Schlüsseldistribution in ViPNet Network Manager.
     - Installieren Sie die Schlüsseldistribution auf den ViPNet Coordinator HW/VA-Knoten.

Achtung! Installieren Sie die Schlüsseldistribution auf einen Knoten, auf dem bereits Schlüssel installiert wurden, nicht neu. Eine Neuinstallation kann Konflikte im VPN-Netzwerk verursachen.

- Wenn eine Schlüsseldistribution auf dem ViPNet Coordinator HW/VA-Knoten bereits installiert wurde, dann führen Sie den Versand der Schlüssel in ViPNet Network Manager durch.

Weitere Informationen zum Erstellen von Schlüsseldistributionen und zum Versand der Schlüssel finden Sie im Dokument „ViPNet VPN. Benutzerhandbuch“.

5 Wenn Sie statische IP-Adressen für den Aufbau von Verbindungen zum Netzwerk benutzen, dann geben Sie auf dem ViPNet Coordinator HW/VA-Knoten manuell die IP-Adressen derjenigen DNS-Server (s. Parameter des DNS-Servers einstellen auf S. 85) und NTP-Server (s. Parameter des NTP-Servers einstellen auf S. 86) an, die verwendet werden sollen.

Wenn Sie eine dynamische IP-Adresse ausgewählt haben, die DNS- und NTP-Server könnte automatisch aus dem DHCP-Server bezogen werden. Prüfen Sie das, indem Sie Liste der verfügbare DNS-Server (s. Parameter des DNS-Servers einstellen auf S. 85) und NTP-Server (s. Parameter des NTP-Servers einstellen auf S. 86) anzeigen. Wenn die Adressen nicht automatisch bezogen wurden, dann geben Sie diese manuell an, indem Sie den Anweisungen in den angegebenen Abschnitten folgen.

Verbinden zu einem Ethernet-Netzwerk mit Hilfe des ViPNet Network Manager

Führen Sie die in diesem Abschnitt beschriebene Schritte auf einem Netzwerkknoten mit dem Programm ViPNet Network Manager.

Hinweis. Die nachfolgenden Schritte können nur dann durchgeführt werden, wenn ViPNet Network Manager der Version 4.1 oder höher installiert ist. Anderenfalls können Sie die Verbindung unter Verwendung der Webschnittstelle (s. Verbindung zum Ethernet-Netzwerk herstellen auf S. 69) oder über die Befehlszeile konfigurieren (s. Aufbau der Verbindung zu einem Ethernet-Netzwerk unter Verwendung der Befehlszeilenschnittstelle auf S. 79).

Führen Sie folgenden Schritte durch, um Ihre ViPNet Coordinator HW/VA an Ethernet-Netzwerk verbinden:

1 Wählen Sie in der Navigationsleiste des Programms ViPNet Network Manager in der Netzwerkknotenliste den benötigten ViPNet Coordinator HW/VA-Knoten aus.

2 Klicken Sie in der Panel-Ansicht auf die Registerkarte **Netzwerkeinstellungen**.

3 Konfigurieren Sie jeden Adapter des Netzwerkknotens auf die folgende Weise:

3.1 Durch Klicken auf die Schaltflächen **Hinzufügen** oder **Bearbeiten** unterhalb des Feldes **Netzwerkadapter** können Sie einen neuen Netzwerkadapter hinzufügen oder einen vorhandenen Netzwerkadapter bearbeiten.

Abbildung 5: Hinzufügen eines neuen Netzwerkadapters

3.2 Wählen Sie im Fenster **Netzwerkadapter** im Feld **Adaptername** den Netzwerkadapter aus, den Sie konfigurieren möchten. Die im System installierten Ethernet-Netzwerkadapter besitzen die Namen `eth0`, `eth1` u. s. w. (abhängig von der Anzahl der Adapter im System).

3.3 Wenn das Kontrollkästchen **Adapter auf dem Gerät aktivieren** deaktiviert ist, dann aktivieren Sie es.

3.4 Konfigurieren Sie die IP-Adresse des Adapters:

- Wenn Sie eine statische IP-Adresse zuweisen möchten, wählen Sie die Option **Statische IP-Adresse verwenden** und geben Sie dann die IP-Adresse und die Maske an.
- Wenn die IP-Adresse automatisch vom DHCP-Server bezogen werden soll, dann wählen Sie die Option **Automatisch (via DHCP)**. Legen Sie bei Bedarf den Bezug der IP-Adresse des Standardgateways vom DHCP-Server fest, indem Sie das entsprechende Kontrollkästchen aktivieren.

- Weisen Sie dem Netzwerkadapter, wenn nötig, IP-Adressaliase zu (s. Zugang zu einem ViPNet Coordinator HW/VA-Knoten durch Zuweisung der IP-Adressen-Aliase bereitstellen auf S. 140). Klicken Sie dazu auf **Hinzufügen** und geben Sie das Alias an.

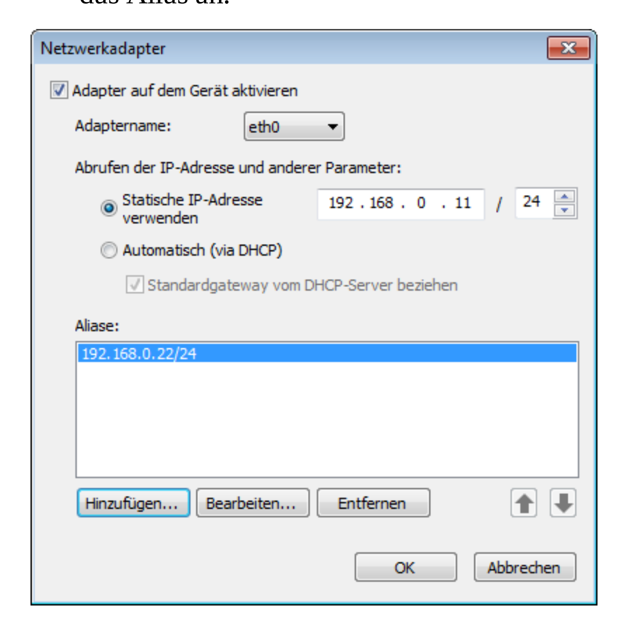


Abbildung 6: Konfiguration eines Netzwerkadapters

3.5 Nachdem Sie die Konfiguration des Adapters fertiggestellt haben, klicken Sie auf **OK**.

4 Geben Sie im Feld **Standardgateway** die IP-Adresse des Standardgateways ein.

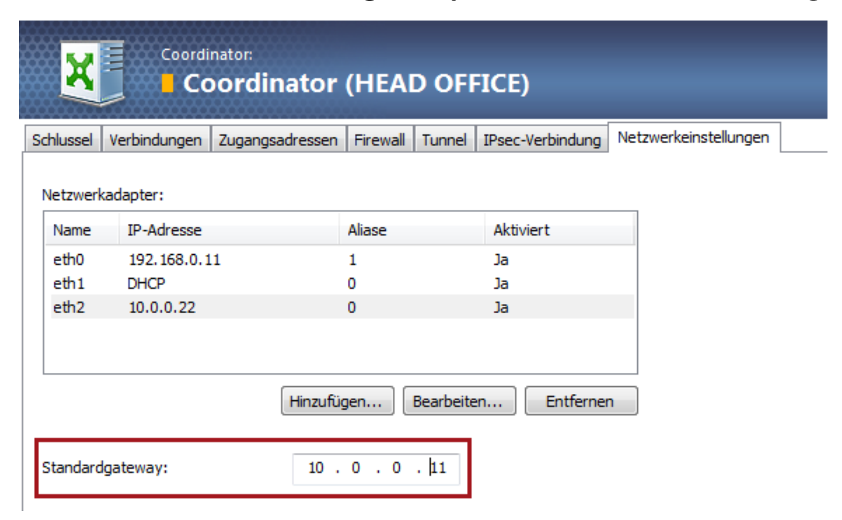


Abbildung 7: Definition des Standardgateways

5 Konfigurieren Sie bei Bedarf die statischen Routen des Knotens. Klicken Sie auf **Hinzufügen** oder **Bearbeiten** unterhalb des Feldes **Statische Routen**, um eine neue statische Route hinzuzufügen oder eine vorhandene Route zu bearbeiten.

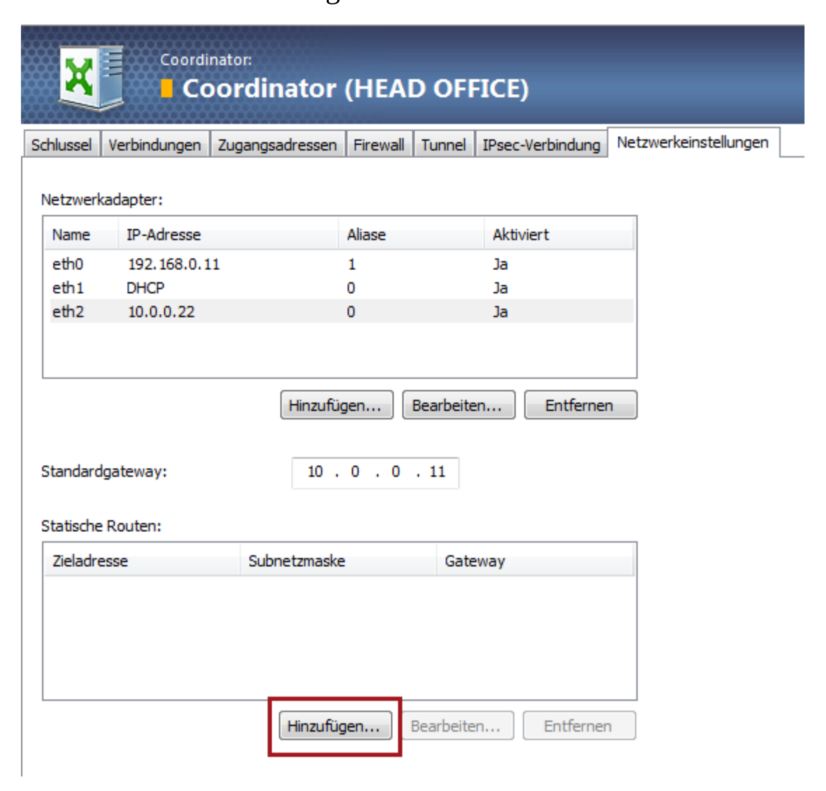


Abbildung 8: Hinzufügen einer neuen statischen Route

Geben Sie im Fenster **Statische Routen** die benötigten Parameter an und klicken Sie auf **OK**.

6 Wählen Sie in der Panel-Ansicht die Registerkarte **Firewall**. Nehmen Sie dort die folgenden Einstellungen vor:

- Wenn der Knoten über eine externe Firewall mit dem Netzwerk verbunden werden soll, dann aktivieren Sie das Kontrollkästchen **Externe Firewall verwenden**. Wählen Sie den erforderlichen Firewalltyp in der Liste aus und konfigurieren Sie bei Bedarf die restlichen Einstellungen.
- Wenn der Knoten direkt (ohne Verwendung einer externen Firewall) mit dem Netzwerk verbunden werden soll, dann deaktivieren Sie das Kontrollkästchen **Externe Firewall verwenden**.

Abbildung 9: Konfiguration der Netzwerkverbindung über eine externe Firewall

Konfiguration der Tunnelung auf einem ViPNet Coordinator HW/VA

Führen Sie die in diesem Abschnitt beschriebene Schritte auf einem Netzwerkknoten mit dem Programm ViPNet Network Manager.

Führen Sie folgenden Schritte durch, um die Tunnelung aud einem ViPNet Coordinator HW/VA einzustellen:

1. Wählen Sie in der Navigationsleiste des Programms ViPNet Network Manager in der Netzwerkknotenliste den ViPNet Coordinator HW/VA-Knoten aus, der die Tunnelung durchführen soll.
2. Klicken Sie in der Panel-Ansicht auf die Registerkarte **Tunnel**.
3. Durch Klicken auf die Schaltflächen **Hinzufügen** oder **Ändern** können Sie eine neue IP-Adresse oder einen Adressbereich zum Tunneln hinzufügen oder eine vorhandene IP-Adresse bzw. Adressbereich bearbeiten.

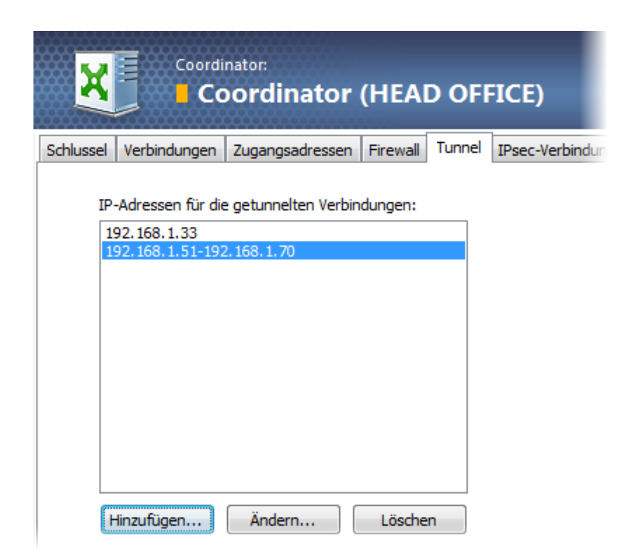


Abbildung 10: Hinzufügen einer getunnelten IP-Adresse

4 Geben Sie im Fenster **IP-Adresse oder Adressbereich** die IP-Adresse oder den Adressbereich an, der getunnelt werden soll, und klicken Sie dann auf **OK**.

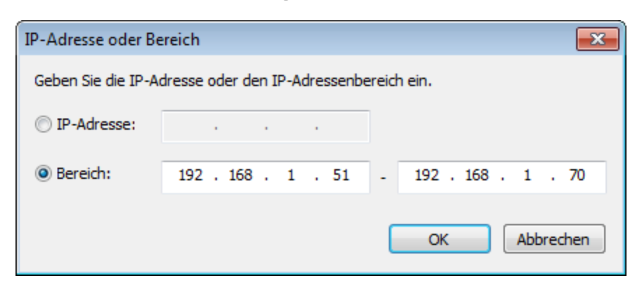


Abbildung 11: Festlegen des Bereichs von getunnelten IP-Adressen

Konfiguration der Netzwerkeinstellungen von ViPNet Coordinator HW/VA mit Hilfe der Webschnittstelle

Achtung! Wenn Sie mit einem Failover-Cluster arbeiten, dann sollten Sie keine Netzwerkeinstellungen über die Webschnittstelle konfigurieren, da die vorgenommenen Einstellungen entweder nicht angewendet werden oder zu Störungen in der Cluster-Konfiguration führen können. Verwenden Sie zum Konfigurieren der Netzwerkeinstellungen auf dem Cluster die Befehlszeilenschnittstelle.

Verbindung zum Ethernet-Netzwerk herstellen

Gehen Sie wie folgt vor, um die Verbindung zu einem Ethernet-Netzwerk zu mit Hilfe der Webschnittstelle konfigurieren:

1. Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an.
2. Klicken Sie auf der Startseite auf **Einstellungen des Netzwerks**.
3. Wählen Sie im linken Bereich der Seite **Netzwerkadapter** den Netzwerkadapter aus, den Sie konfigurieren möchten. Den im Betriebssystem installierten Ethernet-Netzwerkadaptern werden die Namen `eth0`, `eth1`, usw. zugewiesen (in Übereinstimmung mit der Anzahl der Adapter im System).

Abbildung 12: Ethernet-Adaptereinstellungen

4 Stellen Sie sicher, dass der Netzwerkadapter aktiviert ist. Anderenfalls klicken Sie auf den Schalter im oberen Fensterteil. Der Status des Netzwerkadapters wird neben dem Schalter angezeigt.

5 Wählen Sie aus, wie die Verbindung konfiguriert werden soll:

- **Automatisch**: wenn die Verbindungseinstellungen vom DHCP-Server bezogen werden sollen.
- **Manuell**: wenn dem Adapter eine statische IP-Adresse zugewiesen werden soll.

6 Wenn Sie sich entschieden haben, die Verbindung manuell zu konfigurieren:

- Legen Sie in den entsprechenden Feldern die IP-Adresse und die Netzwerkmaske für den Netzwerkadapter fest. Klicken Sie dann auf **Speichern**.
- Geben Sie die IP-Adressen der DNS-Server (s. Parameter des DNS-Servers einstellen auf S. 85) und NTP-Server (s. Parameter des NTP-Servers einstellen auf S. 86), die Sie verwenden möchten, an.

Hinweis. Wenn Sie die automatische Konfiguration ausgewählt haben, können die IP-Adressen der DNS- und NTP-Server vom DHCP-Server bezogen werden.

7 Wenn nötig, ändern Sie die Routingtabelle des Knotens (s. Ändern der Routingtabelle auf S. 77).

8 Wenn nötig, weisen Sie dem Netzwerkadapter IP-Adressen-Aliase zu (s. Zuweisung der IP-Adressen-Aliase auf S. 76).

Verbindung zum Wi-Fi-Netzwerk herstellen

Wenn Ihr ViPNet Coordinator HW/VA über einen Wi-Fi-Adapter verfügt, können Sie Verbindungen zu einem Drahtlosnetzwerk aufbauen.

Hinweis. Ein ViPNet Coordinator HW/VA-Knoten kann auch als ein Access Point auftreten. Die gleichzeitige Verwendung als Client und als Access Point wird von ViPNet Coordinator HW/VA jedoch nicht unterstützt.

Gehen Sie wie folgt vor, um die Verbindung zu einem Wi-Fi-Netzwerk als Client zu konfigurieren:

1 Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).

2 Klicken Sie auf der Startseite auf **Netzwerkdienste**. Die Seite **Netzwerkadapter** wird geöffnet.

3 Wählen Sie im linken Bereich den Wi-Fi-Netzwerkadapter aus. Einem im Betriebssystem installierten Wi-Fi-Adapter wird der Name `wlan0` zugewiesen.

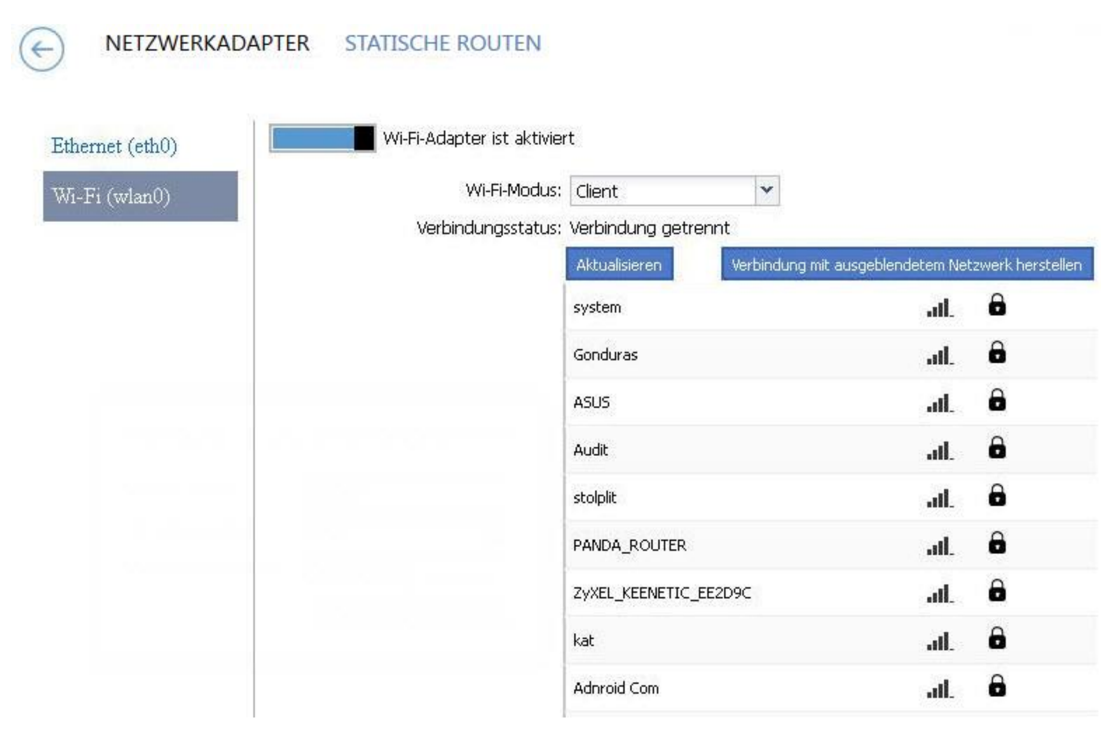


Abbildung 13: Aufbau der Verbindung mit einem Wi-Fi-Netzwerk

4 Stellen Sie sicher, dass der Wi-Fi-Adapter aktiviert ist. Anderenfalls klicken Sie auf den Schalter im oberen Fensterteil. Der Status des Netzwerkadapters wird neben dem Schalter angezeigt.

5 Wählen Sie in der Liste **Wi-Fi-Modus** den Eintrag **Client**. Eine Liste aller verfügbaren Wi-Fi-Netzwerke wird angezeigt.

Gesicherte Netzwerke sind durch das Symbol gekennzeichnet. Netzwerke, deren Authentifizierungstyp nicht unterstützt wird, sind durch das Symbol gekennzeichnet. Klicken Sie auf **Aktualisieren**, um die Liste der verfügbaren Netzwerke zu aktualisieren.

6 Wählen Sie in der Liste der verfügbaren Wi-Fi-Netzwerke das benötigte Netzwerk aus und klicken Sie auf **Verbinden**.

7 Wenn das Netzwerk gesichert ist, geben Sie im eingeblendeten Fenster **Verbindung zum <Netzwerkname>** das Netzwerkpasswort ein und klicken Sie dann auf **Verbinden**.

Wenn Sie sich zu einem versteckten Wi-Fi-Netzwerk verbinden möchten und den Namen dieses Netzwerks sowie den Sicherheitsschlüssel kennen, dann gehen Sie wie folgt vor:

1 Wählen Sie auf der Wi-Fi-Konfigurationsseite den Client-Verbindungsmodus (s. oben).

2 Klicken Sie auf **Verbindung zum ausgeblendetem Netzwerk herstellen**.

3 Geben Sie im Fenster **Verbindung zum ausgeblendetem Netzwerk** den Namen, den Verschlüsselungstyp und das Passwort für das Netzwerk an, zu dem Sie eine Verbindung aufbauen möchten.

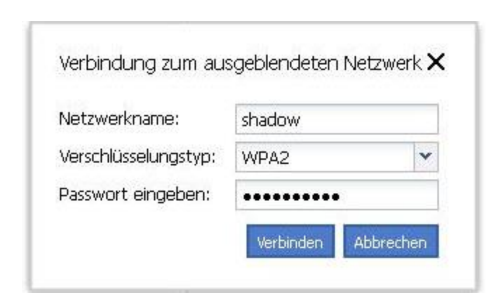


Abbildung 14: Aufbau der Verbindung mit einem verborgenen Netzwerk

4 Klicken Sie auf **Verbinden**.

Herstellen der Verbindung zu einem mobilen 3G/LTE-Netzwerk

ViPNet Coordinator HW/VA kann sich über 3G- bzw. LTE-Mobilfunknetze mit Hilfe eines USB-Modems zum Internet verbinden. Im System wird ein 3G- bzw. LTE-Modem als Netzwerkadapter mit dem Namen `pppX` abgebildet.

Für Verbindungen zum Internet können die Dienste eines beliebigen Mobilfunkanbieters genutzt werden. Dazu sind die Anschaffung einer SIM-Karte und die Aktivierung entsprechender Dienste (falls nötig) erforderlich. Ausführliche Informationen über die Bedingungen eines Internet-Anschlusses können Sie bei Ihrem Mobilfunkanbieter anfordern.

Achtung! Eine Appliance, für die der Internetzugang über ein 3G/LTE-Modem konfiguriert wurde, kann nicht gleichzeitig über einen anderen Adapter (Ethernet oder Wi-Fi) auf das Internet zugreifen.

Gehen Sie wie folgt vor, um die Verbindung mit einem mobilen Netzwerk herzustellen:

1 Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).

2 Stellen Sie sicher, dass keinem der Netzwerkadapter der Appliance Standard-Gateways zugewiesen werden (manuell oder über DHCP):

2.1 Klicken Sie auf der Startseite auf **Einstellungen des Netzwerks**.

2.2 Wählen Sie auf der Seite **Netzwerkadapter** in der linken Leiste jeden einzelnen Adapter nacheinander aus und stellen Sie sicher, dass die Verbindung jedes Adapters automatisch (über DHCP) konfiguriert wird.

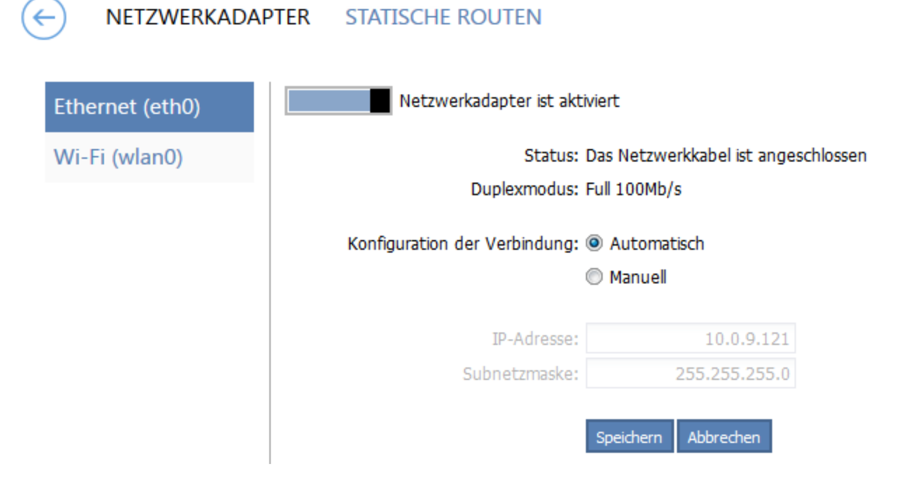


Abbildung 15: Parameter des Netzwerkadapters prüfen

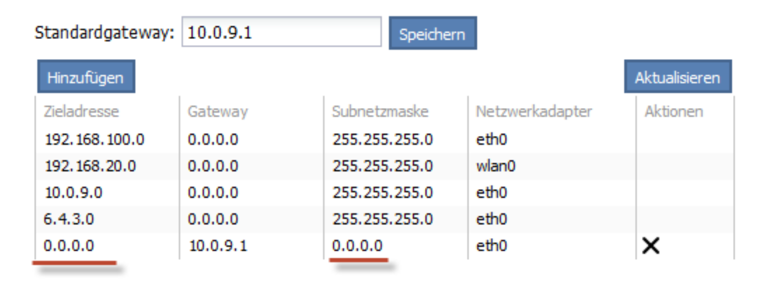
Wenn die Verbindung automatisch konfiguriert wird (in Gruppe **Konfiguration der Verbindung** ist die Option **Automatisch** ausgewählt), dann führen Sie eine der folgenden Aktionen durch:

- deaktivieren Sie den Adapter, indem Sie auf den Schalter im oberen Seitenbereich klicken,
- wählen Sie in Gruppe **Konfiguration der Verbindung** die Option **Manuell** aus und klicken auf **Speichern**.

2.3 Klicken Sie auf der Seite **Statische Routen** auf die Schaltfläche **Aktualisieren**.

2.4 Überprüfen Sie, ob die Tabelle Standardgateway-Einträge enthält. Falls solche Einträge vorhanden sind, löschen Sie diese, indem Sie auf das Symbol ✕ und dann auf **OK** klicken.

Beim Standardgateway-Eintrag sind für die **Zieladresse** und die **Subnetzmaske** die Werte `0.0.0.0.` eingetragen.



Standardgateway: 10.0.9.1 Speichern

Hinzufügen Aktualisieren

Zieladresse	Gateway	Subnetzmaske	Netzwerkadapter	Aktionen
192.168.100.0	0.0.0.0	255.255.255.0	eth0	
192.168.20.0	0.0.0.0	255.255.255.0	wlan0	
10.0.9.0	0.0.0.0	255.255.255.0	eth0	
6.4.3.0	0.0.0.0	255.255.255.0	eth0	
0.0.0.0	10.0.9.1	0.0.0.0	eth0	✕

Abbildung 16: Standardgateway wird in der Tabelle angezeigt

2.5 Kehren Sie zur Startseite zurück, indem Sie auf ⓔ links oben klicken.

3 Aktivieren Sie das Modem:

3.1 Schließen Sie das 3G/LTE-Modem an einen USB-Port der Appliance an.

3.2 Klicken Sie auf der Homepage auf **Einstellungen des Netzwerks**.

3.3 Wählen Sie auf der Seite **Netzwerkadapter** in der linken Leiste den Modemadapter aus, den Sie konfigurieren möchten.

3.4 Wählen Sie Ihren Mobilfunkanbieter in der Liste **Mobilfunkanbieter** aus.

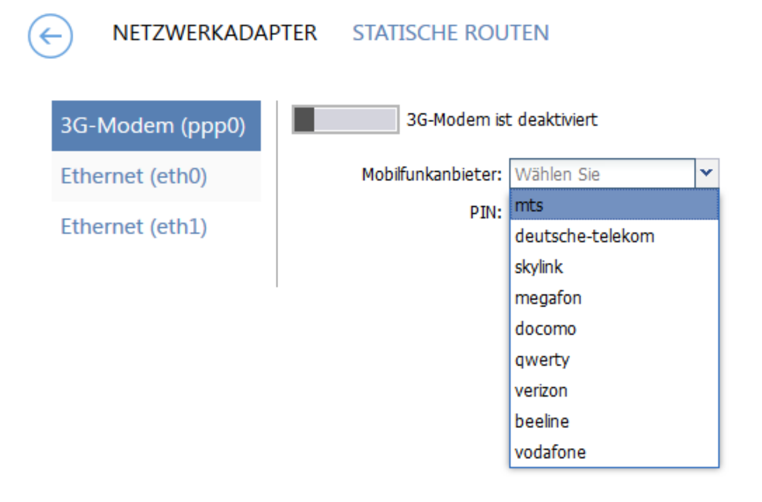


Abbildung 17: 3G/LTE-Modem konfigurieren

3.5 Falls die SIM-Karte mit einer PIN geschützt ist, geben Sie den PIN-Code im Eingabefeld **PIN** ein.

3.6 Klicken Sie zum Speichern der Einstellungen auf **Speichern**.

3.7 Aktivieren Sie das Modem, indem Sie auf den Schalter im oberen Seitenbereich klicken.

3.8 Kehren Sie zur Startseite zurück, indem Sie auf ⓔ links oben klicken.

4 Konfigurieren Sie die integrierte Firewall, damit Knoten im LAN, die sich hinter einem Coordinator befinden, über die 3G/LTE-Verbindung auf das Internet zugreifen können.

Wenn Ihre Coordinator HW-Plattform keine Proxyserver-Funktionalität unterstützt (s. ViPNet Coordinator HW Hardware-Appliances auf S. 12), dann konfigurieren Sie Proxy-Server (s. Konfiguration der allgemeinen Proxyserver-Einstellungen auf S. 91), und die integrierte Firewall wird automatisch konfiguriert.

Andernfalls können Sie den Proxyserver manuell konfigurieren (s. Manuelle Konfiguration der integrierten Firewall für den Zugruiff des Netzwerkknoten ins Internet aus lokalem Netzwerk auf S. 167).

5 Nehmen Sie auf den Computern, die unter Verwendung der Appliance auf das Internet zugreifen, die folgenden Einstellungen vor:

   - Wenn Sie den transparenten Proxyservermodus aktiviert haben, dann legen Sie die Appliance als Standardgateway des Computers fest.
   - Wenn Sie den transparenten Proxyservermodus nicht aktiviert haben, dann legen Sie die Appliance im Webbrowser als Proxyserver fest. Verwenden Sie dazu die IP-Adresse und den Port der Appliance, die zum Abhören des entsprechenden Netzwerks verwendet werden.

Zuweisung der IP-Adressen-Aliase

Die Zuweisung der IP-Adressen-Aliase an die Netzwerkadapter kann für die Implementierung einer Vielzahl an Netzwerktopologien sinnvoll sein (s. Zugang zu einem ViPNet Coordinator HW/VA-Knoten durch Zuweisung der IP-Adressen-Aliase bereitstellen auf S. 140).

Gehen Sie wie folgt vor, um einem Netzwerkadapter einen IP-Adressen-Alias zuzuweisen:

1 Melden Sie sich über die Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).

2 Klicken Sie auf der Homepage auf **Einstellungen des Netzwerks**.

3 Wählen Sie auf der Seite **Netzwerkadapter** in der linken Leiste den Netzwerkadapter aus, den Sie konfigurieren möchten.

4 Zum Hinzufügen eines IP-Adresses-Alias zum Netzwerkadapter:

   - Klicken Sie unter **Aliase für eth** auf **Hinzufügen**.
   - Geben Sie in der neuen Zeile die erforderliche IP-Adresse und die Netzwerkmaske an, die Sie dem Netzwerkadapter zuweisen möchten. Klicken Sie dann auf **Speichern**.

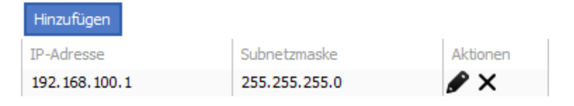


Abbildung 18: IP-Adressaliase

5 Zum Ändern eines IP-Adressen-Alias:

   - Doppelklicken Sie auf den Eintrag des Alias, den Sie ändern möchten.
   - Ändern Sie die IP-Adresse und die Netzwerkmaske und klicken Sie dann auf **Speichern**.

6 Zum Löschen eines IP-Adressen-Alias:

- Klicken Sie im Eintrag des Alias, den Sie löschen möchten, auf das Symbol ✕.
- Klicken Sie im Meldungsfenster auf **OK**. Der Alias wird gelöscht.

Ändern der Routingtabelle

Wenn erforderlich, können Sie die Routingtabelle eines ViPNet Coordinator HW/VA-Knotens ändern. Dazu:

1. Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).
2. Klicken Sie auf der Startseite auf **Netzwerkdienste**.
3. Klicken Sie im oberen Fensterteil auf **Routing**.

   Die Routingtabelle kann Routen enthalten, die entweder automatisch für jeden Netzwerkadapter hinzugefügt oder vom Benutzer definiert wurden. Automatisch hinzugefügte Routen können nicht geändert oder gelöscht werden.

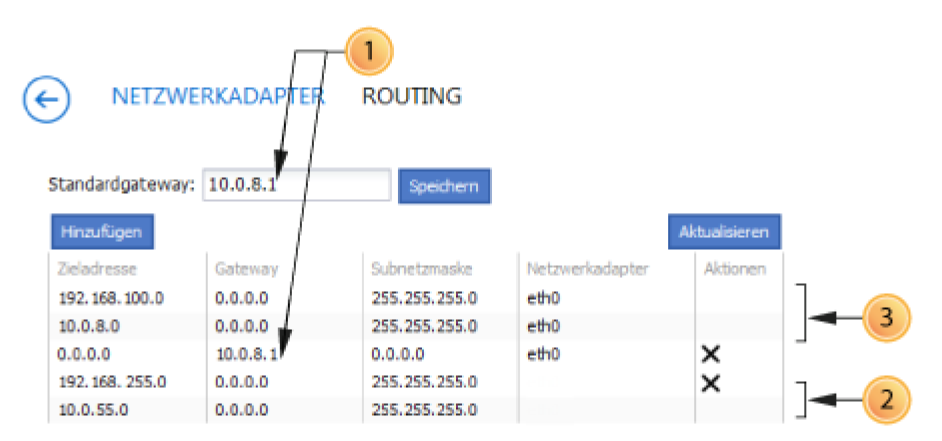


Abbildung 19: Routingtabelle

1. Standardgateway.

2. Benutzerdefiniete Routen.

3. Für jeden Netzwerkadapter und seinen Alias automatisch hinzugefügte Routen. Diese werden anhand der IP-Adressen der Adapter ermittelt und können weder geändert noch gelöscht werden. Im oben angeführten Beispiel besitzen die Adapter die folgenden IP-Adressen:

- `eth0:` `10.10.10.2`
- `eth0 alias:` `192.168.100.1`
- `eth1:` `192.168.125.160`

Hinweis. Wenn keine Routen in der Tabelle angezeigt werden, dann aktualisieren Sie die Tabelle durch einen Klick auf **Aktualisieren**.

4 Wenn Sie das Standardgateway hinzufügen oder ändern möchten, dann geben Sie im entsprechenden Feld seine IP-Adresse ein und klicken Sie dann auf **Speichern**.

   Der Standardgateway-Eintrag in der Routingtabelle wird entsprechend geändert.

5 Zum Hinzufügen einer neuen Route:
   - Klicken Sie auf **Hinzufügen**.
   - Geben Sie die Ziel-IP-Adresse, ein Gateway, das für den Zugriff auf die Zieladresse verwendet wird, und eine Subnetzmaske an.

     Ein Netzwerkadapter wird automatisch definiert.
   - Klicken Sie auf **Speichern**.

6 Zum Ändern einer Route:
   - Doppelklicken Sie auf die Zeile mit der Route, die Sie ändern möchten.
   - Ändern Sie die Eigenschaften der Route.
   - Klicken Sie auf **Speichern**.

7 Zum Löschen einer Route:
   - Klicken Sie in der Zeile der Route, die Sie löschen möchten, auf das Symbol ✕.
   - Klicken Sie im Meldungsfenster auf **OK**. Die Route wird gelöscht.

Aufbau der Verbindung zu einem Ethernet-Netzwerk unter Verwendung der Befehlszeilenschnittstelle

Wenn der Zugriff auf den ViPNet Coordinator HW/VA-Knoten aus dem Netzwerk nicht möglich ist, dann kann die Knotenverbindung lokal unter Verwendung der Befehlszeilenschnittstelle konfiguriert werden.

Tipp. Es ist ausreichend, nur einen Netzwerkadapter lokal zu konfigurieren. Nachdem dieser Adapter konfiguriert ist, kann der Knoten über das Netzwerk angesprochen werden, und Sie können die restlichen Parameter des Knotens remote über eine benutzerfreundliche Webschnittstelle konfigurieren (s. Konfiguration der Netzwerkeinstellungen von ViPNet Coordinator HW/VA mit Hilfe der Webschnittstelle auf S. 69).

Verwenden Sie beim Konfigurieren eines Ethernet-Adapters den jeweiligen Adapternamen. Die Ethernet-Adapter besitzen die Namen `eth0`, `eth1`, u. s. w.

Führen Sie folgende Schritte durch, um Netzwerkadapter zu konfigurieren:

1. Wechseln Sie in der Befehlszeilenschnittstelle in den Administratormodus mit Hilfe des Befehls `enable`.
2. Aktivieren Sie den Adapter, indem Sie den folgenden Befehl ausführen:

   `inet ifconfig <Adaptername> up`

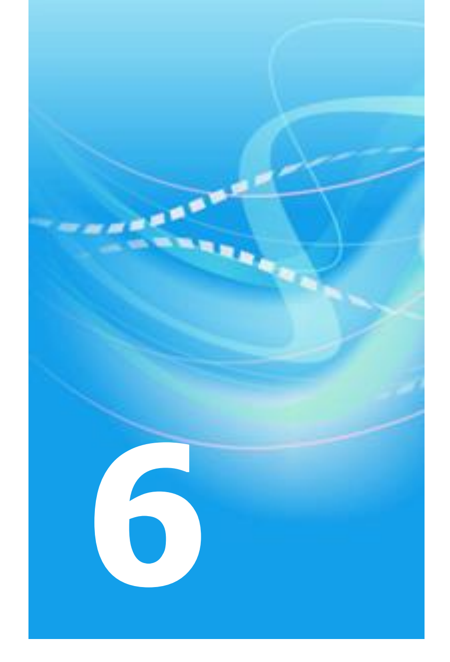
3. Wählen Sie dann eine der folgenden Optionen aus:
   - Wenn die Verbindungseinstellungen von einem DHCP-Server bezogen werden sollen, dann führen Sie den Befehl `inet ifconfig <Adaptername> dhcp` aus.
   - Wenn Sie die Verbindungseinstellungen manuell vornehmen möchten, dann:
     - legen Sie die IP-Adresse und die Netzwerkmaske des Adapters fest, indem Sie den Befehl `inet ifconfig <Adaptername> address <IP-Adresse> netmask <Netzwerkmaske>` ausführen;

- legen Sie das Standardgateway des Adapters fest, indem Sie den Befehl `inet route add default gw <Gateway-IP-Adresse>` ausführen.

Beispiel der Befehlsverwendung:

```
inet ifconfig eth0 up
inet ifconfig eth0 address 10.0.8.79 netmask 255.255.255.0
inet route add default gw 10.0.8.1
```

Weitere Informationen zur lokalen Konfiguration der Netzwerkadapter s. Dokument „ViPNet Coordinator HW/VA. Referenzhandbuch".



Konfiguration der integrierten Dienste

Parameter für Netzwerkdienste einstellen

Auf ViPNet Coordinator HW/VA-Appliance können mehrere Netzwerkdienste ausgeführt werden, die in einem lokalen Netzwerk von Nutzen sind und den Betrieb eines kleinen Firmennetzwerks erleichtern.

Parameter des Wi-Fi-Access Points einstellen

Wenn das Appliance über einen Wi-Fi-Adapter verfügt, kann ViPNet Coordinator HW/VA als Wi-Fi-Zugriffspunkt verwendet werden.

Hinweis. Ein ViPNet Coordinator HW/VA-Knoten kann auch als ein Wi-Fi-Client auftreten (s. Verbindung zum Wi-Fi-Netzwerk herstellen auf S. 71). Die gleichzeitige Verwendung als Client und als Access Point wird von ViPNet Coordinator HW/VA jedoch nicht unterstützt.

Wenn der Wi-Fi-Zugriffspunkt aktiviert ist, wird dem Netzwerkadapter automatisch die IP-Adresse 192.168.20.1 zugewiesen. Auf diesem Adapter wird ein DHCP-Server gestartet. Der DHCP-Server verfügt über fixe Parameter, die nicht vom Benutzer geändert werden können:

- Bereich der zu verteilenden IP-Adressen: 192.168.20.2–192.168.20.20.
- Adresse des DNS- und NTP-Servers: 192.168.20.1 (Adresse des Netzwerkadapters `wlan0`).

Wenn Sie ViPNet Coordinator HW/VA als Wi-Fi-Zugriffspunkt einstellen möchten:

1. Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).
2. Klicken Sie auf der Startseite auf **Einstellungen des Netzwerks**.
3. Wählen Sie den Wi-Fi-Netzwerkadapter im linken Bereich der Seite **Netzwerkadapter** aus. Einem im Betriebssystem installierten Wi-Fi-Adapter wird der Name `wlan0` zugewiesen.

4 Stellen Sie sicher, dass der Wi-Fi-Adapter aktiviert ist. Anderenfalls klicken Sie auf den Schalter im oberen Fensterteil. Der Status des Netzwerkadapters wird neben dem Schalter angezeigt.

5 Wählen Sie in der Liste **Wi-Fi-Modus** den Eintrag **Zugriffspunkt**.

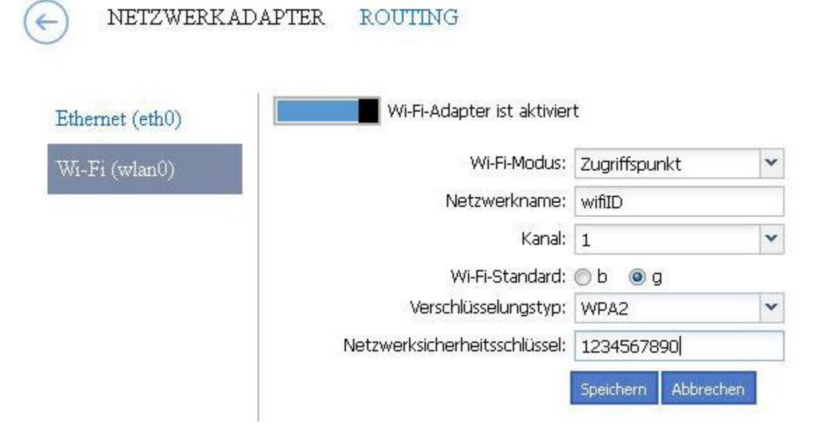


Abbildung 20: Konfiguration eines Wi-Fi-Access Point

6 Geben Sie im Feld **Netzwerkname** den Namen Ihres Wi-Fi-Netzwerks an.

7 Wählen Sie in der Liste **Kanal** die Nummer des Wi-Fi-Kanals aus, die vom konfigurierten Access Point verwendet werden soll.

Legen Sie in Gruppe **Wi-Fi-Standard** den Verbindungsstandard für Ihr drahtloses Netzwerk fest. Folgende Standards werden unterstützt:

- **b** (IEEE 802.11b): 2.4 GHz, Verbindungsgeschwindigkeit bis zu 11 Mbit/Sek.
- **g** (IEEE 802.11g): 2.4 GHz, Verbindungsgeschwindigkeit bis zu 54 Mbit/Sek.

8 Wählen Sie in der Liste **Verschlüsselungstyp** den Typ der Verschlüsselung für die Benutzerauthentifizierung aus:

- Wenn Sie den Wert **Keine Verschlüsselung** auswählen, werden die Benutzer in der Lage sein, sich ohne Eingabe eines Passworts mit dem Netzwerk zu verbinden.
- Wenn Sie den Wert **WPA** oder **WPA2** auswählen, dann geben Sie im Feld **Netzwerksicherheitsschlüssel** ein Passwort ein, das die Benutzer für ihre Authentifizierung verwenden sollen. Leiten Sie dieses Passwort an alle Benutzer weiter, die in der Lage sein sollen, sich zu Ihrem Wi-Fi-Netzwerk zu verbinden.

9 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

10 Damit Verbindungen zwischen den Geräten innerhalb des Wi-Fi-Netzwerks und den Computern in Ihrem Ethernet-Netzwerk möglich sind, konfigurieren Sie auf dem ViPNet Coordinator HW/VA-Knoten in der Firewall-Konfigurationsdatei Weiterleitungsregeln,

die den Austausch der IP-Pakete zwischen den beiden Netzwerken erlauben (s. Bearbeitungsregeln für offenen Traffic einstellen auf S. 110).

Parameter des DHCP-Servers einstellen

ViPNet Coordinator HW/VA kann im lokalen Netzwerk als DHCP-Server auftreten (s. DHCP-Server auf S. 243). Wenn der Netzwerkknoten mit installiertem ViPNet Coordinator HW/VA als Wi-Fi-Access Point (s. Parameter des Wi-Fi-Access Points einstellen auf S. 82) eingesetzt wird, dann wird auf dem entsprechenden Netzwerkadapter automatisch ein DHCP-Server gestartet, dessen Parameter nicht vom Benutzer geändert werden können.

Wenn der DHCP-Server auf einem der Ethernet-Netzwerkadapter gestartet werden soll, müssen die Parameter dieses Servers manuell konfiguriert werden. Führen Sie dazu die folgenden Schritte aus:

1 Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).

2 Klicken Sie auf der Startseite auf **Netzwerkdienste**.

3 Klicken Sie im oberen Fensterteil auf **DHCP-Server**.

Abbildung 21: Konfiguration der DHCP-Servereinstellungen

4 Wählen Sie in der Liste **Netzwerkadapter** den Ethernet-Netzwerkadapter aus, auf dem der DHCP-Server ausgeführt werden soll.

Hinweis. Der DHCP-Server kann nur an einem Adapter verwendet werden, der eine IP-Adresse aus dem privaten Netzwerkbereich besitzt: 10.0.0.0/8, 172.16.0.0/12 oder 192.168.0.0/16.

5 Definieren Sie in den **Bereich der verteilten IP-Adressen** die Start- und End-IP-Adresse für den Adressenbereich, aus dem Adressen an DHCP-Clients vergeben werden sollen.

6 Geben Sie im Feld **Gateway** die IP-Adresse des Standardgateways an. Diese Gateway-Adresse wird von den DHCP-Clients vom Server abgerufen.

7 Legen Sie in Gruppe **IP-Adressen-Leasezeitraum** den Zeitraum für die Gültigkeit der vergebenen IP-Adressen fest:

   - Wählen Sie die Zeiteinheiten für den Leasezeitraum aus: **Tage** oder **Stunden**.
   - Geben Sie die Länge des Zeitintervalls in Tagen (**Tage**) oder Stunden (**Stunden**) ein.

8 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

9 Klicken Sie auf den Schalter im oberen Fensterteil, um den DHCP-Server zu starten. Der Status des DHCP-Servers wird neben dem Schalter angezeigt.

Parameter des DNS-Servers einstellen

ViPNet Coordinator HW/VA kann im lokalen Netzwerk als DNS-Server auftreten (s. DNS-Server auf S. 243). Der eingebaute DNS-Server von ViPNet Coordinator HW/VA leitet die eingehenden DNS-Anfragen an den übergeordneten DNS-Server um und übermittelt die erhaltenen Antworten an die Clients. Standardmäßig werden Clientanfragen an DNS-Stammserver umgeleitet.

Sie können eine benutzerdefinierte Liste der DNS-Server festlegen, an welche die DNS-Anforderungen weitergeleitet werden sollen. Der ViPNet Coordinator HW/VA-Knoten sendet seine DNS-Anforderungen an die Server in der Liste, und zwar auch dann, wenn der integrierte DNS-Server deaktiviert ist.

Zum Konfigurieren des DNS-Servers:

1 Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).

2 Klicken Sie auf der Startseite auf **Netzwerkdienste**.

3 Klicken Sie im oberen Fensterteil auf **DNS-Server**.

   Die Liste der DNS-Server auf der Seite **DNS-Server** kann sowohl benutzerdefinierte Serveradressen als auch IP-Adressen, die von einem DHCP-Server automatisch bezogen wurden, enthalten. Der Typ des jeweiligen DNS-Servers wird in Spalte **Typ** angezeigt. Automatisch bezogene Server-IP-Adressen können nicht gelöscht oder geändert werden.

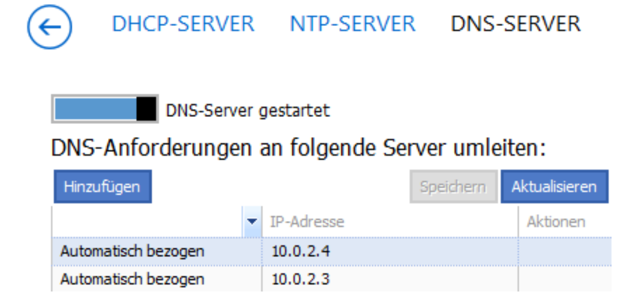


Abbildung 22: Konfiguration der DNS-Einstellungen

4 Klicken Sie auf den Schalter im oberen Fensterteil, um den integrierten DNS-Server zu starten oder zu stoppen. Der Status des DNS-Servers wird neben dem Schalter angezeigt.

5 Zum Hinzufügen der IP-Adresse eines DNS-Servers zur Liste:

- Klicken Sie auf **Hinzufügen**.
- Geben Sie die IP-Adresse des DNS-Servers, den Sie hinzufügen möchten, in der neuen Zeile ein.
- Drücken Sie die **Eingabe**-Taste.

6 Zum Ändern der IP-Adresse eines DNS-Servers:

- Klicken Sie auf die IP-Adresse, die Sie ändern möchten.
- Ändern Sie die Adresse.
- Drücken Sie die **Eingabe**-Taste.

7 Zum Löschen der IP-Adresse eines DNS-Servers aus der Liste:

- Klicken Sie in der Zeile der DNS-Serveradresse, die Sie löschen möchten, auf das Symbol ✕.
- Klicken Sie im Meldungsfenster auf **OK**. Die Adresse des DNS-Servers wird gelöscht.

Parameter des NTP-Servers einstellen

ViPNet Coordinator HW/VA kann im lokalen Netzwerk als NTP-Server auftreten (s. NTP-Server auf S. 246). Der eingebaute NTP-Server synchronisiert automatisch die Systemzeit mit der Weltzeit, um Clients mit korrekten Zeitwerten versorgen zu können. Standardmäßig wird der Server `pool.ntp.org` für die Synchronisierung verwendet.

Sie können eine benutzerdefinierte Liste der NTP-Server festlegen, die für die Synchronisierung der Systemzeit von ViPNet Coordinator HW/VA verwendet werden. Die Synchronisierung wird auch dann durchgeführt, wenn der integrierte NTP-Server deaktiviert ist.

Zum Konfigurieren des NTP-Servers:

1 Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).

2 Klicken Sie auf der Startseite auf **Netzwerkdienste**.

3 Klicken Sie im oberen Fensterteil auf **NTP-Server**.

   Die Liste der NTP-Server auf der Seite **NTP-Server** kann sowohl benutzerdefinierte Server als auch Serveradressen, die von einem DHCP-Server automatisch bezogen wurden, enthalten. Der Typ des jeweiligen NTP-Servers wird in Spalte **Typ** angezeigt. Automatisch bezogene Server-IP-Adressen können nicht gelöscht oder geändert werden.

Hinweis. Der Standardserver `pool.ntp.org` wird in der Liste nicht angezeigt.

Abbildung 23: Konfiguration der NTP-Einstellungen

4 Klicken Sie zum Starten oder Anhalten des integrierten NTP-Servers auf den Schalter im oberen Bereich der Seite. Wenn sich der NTP-Server mit keinem der angegebenen Server sowie dem Standardserver synchronisieren konnte, dann wird der NTP-Server automatisch angehalten.

   Der Status des NTP-Servers wird neben dem Schalter angezeigt.

Achtung! Der Standardserver und alle Server in der Tabelle, die mit ihren DNS-Namen angegeben sind, sind nur dann zugänglich, wenn der DNS-Server gestartet ist (s. Parameter des DNS-Servers einstellen auf S. 85).

5 Zum Hinzufügen eines NTP-Servers zur Liste:

   - Klicken Sie auf **Hinzufügen**.

- Geben Sie die IP-Adresse oder den DNS-Namen des NTP-Servers, den Sie hinzufügen möchten, in der neuen Zeile ein.
- Drücken Sie die **Eingabe**-Taste.

6 Zum Ändern der IP-Adresse oder des DNS-Namens eines NTP-Servers:

- Klicken Sie auf den NTP-Server, den Sie ändern möchten.
- Ändern Sie die IP-Adresse oder den DNS-Namen.
- Drücken Sie die **Eingabe**-Taste.

7 Zum Löschen eines NTP-Servers aus der Liste:

- Klicken Sie in der Zeile des NTP-Servers, den Sie löschen möchten, auf das Symbol ✕.
- Klicken Sie im Meldungsfenster auf **OK**. Der NTP-Server wird gelöscht.

Konfiguration des Proxy-Servers

Ein Proxyserver gewährleistet die sichere Arbeit der Firmennetzwerk-Benutzer im Internet durch Kontrolle des Zugangs zu unterschiedlichen Internetobjekten. Wenn der Benutzer auf irgendein Internetobjekt über das HTTP- oder FTP-Protokoll zugreift, dann wird seine Anfrage zunächst vom Proxyserver verarbeitet. Der Proxyserver kann dabei entweder die angefragten Daten laden und an den Benutzer weiterleiten oder den Zugriff verweigern.

Der Proxyserver, der Teil der Softwarelösung ViPNet Coordinator HW/VA ist, verfügt über die folgenden funktionellen Möglichkeiten:

- Caching von Daten, um den Zugang der Benutzer zu häufig verwendeten Objekten zu beschleunigen.
- Möglichkeit, im transparenten Modus zu arbeiten. Dazu sind keine weiteren Einstellungen in den Client-Anwendungen erforderlich.
- Kontrolle des Inhalts von Internetobjekten (s. Inhaltskontrolle konfigurieren auf S. 94).
- Kontrolle des Inhalts von Internetobjekten mit Hilfe einer Antivirus-Prüfung (s. Antivirus konfigurieren auf S. 97).

Hinweis. Proxyserver einschließlich Antivirus und Inhaltsfilter werden von ViPNet Coordinator HW der Modifikationen HW 100 X1/X4/X5/X6 nicht unterstützt.

Das Funktionsschema des Proxyservers bei Verarbeitung einer Benutzeranfrage wird in der folgenden Abbildung dargestellt.

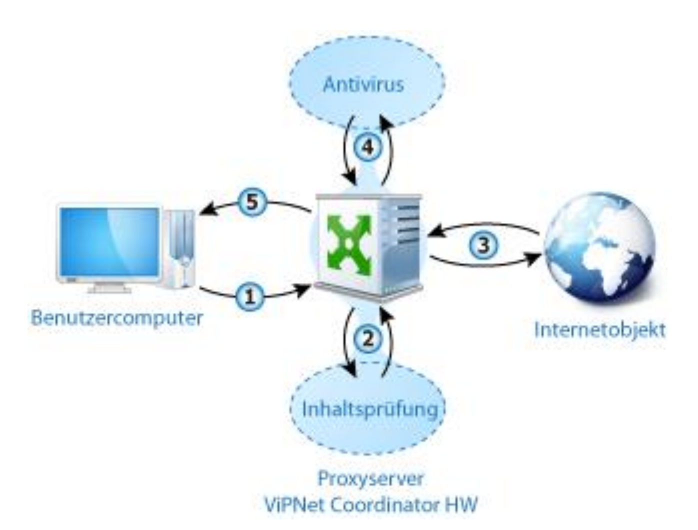


Abbildung 24: Funktionsschema des Proxyservers mit Inhaltsprüfung und Antivirus

Beim Zugriffsversuch des Benutzers auf irgendein Internetobjekt wird die Benutzeranfrage folgendermaßen verarbeitet:

1 Anfrage trifft auf dem Proxyserver ein.

2 Wenn die Funktion der Inhaltsprüfung aktiviert ist, wird die Adresse des Objekts mit der Datenbank blockierter IP-Adressen verglichen.

3 Wenn das Objekt nicht blockiert ist, lädt der Proxyserver die Daten aus dem Internet.

4 Wenn die Antivirus-Funktionalität aktiviert ist, dann werden die geladenen Daten vom Antivirus-Modul geprüft.

5 Falls die Prüfung erfolgreich verläuft, werden die Daten an den Benutzer weitergeleitet.

Falls bei irgendeinem dieser Schritte der Datenzugang blockiert wird, erhält der Benutzer eine entsprechende Meldung.

Wenn das Firmennetzwerk mehrere lokale Netzwerke umfasst, dann können alle diese Netzwerke von einem zentralen Proxyserver auf Basis von ViPNet Coordinator HW/VA bedient werden. In diesem Fall leiten ViPNet Coordinator HW/VA-Server, die sich in lokalen Netzwerken befinden, alle Benutzeranfragen an den zentralen Proxyserver weiter. Der Proxyserver führt anschließend die Verarbeitung dieser Anfragen durch. Weitere Details s. Abschnitt Zentralen Proxyserver verwenden (s. Zentralisierten Proxyserver verwenden auf S. 144).

Konfiguration der allgemeinen Proxyserver-Einstellungen

Wenn Sie den Internetzugang für Ihre lokalen Benutzer absichern möchten, indem Sie den integrierten Proxyserver aktivieren, dann sollten Sie zunächst die allgemeinen Parameter des Proxyservers konfigurieren. Optional können Sie Inhaltsfilter einstellen und den Antivirusschutz aktivieren. Weitere Informationen dazu s. Inhaltskontrolle konfigurieren (auf S. 94) und Antivirus konfigurieren (auf S. 97).

Die Konfiguration der Basisparameter besteht darin, den externen Netzwerkadapter des Servers, die abzuhörende IP-Adresse und die IP-Adressen der lokalen Netzwerke, die den Proxyserver verwenden sollen, zu definieren. Zusätzlich können Sie den transparenten Modus auf dem Proxyserver aktivieren.

Wenn der Proxyserver als „nicht transparenter" Proxy auftritt (d. h. der transparente Modus ist deaktiviert), sollten Sie die IP-Adresse und den Port des Proxyservers in Benutzerprogrammen (Webbrowser) aktivieren.

Wenn der Proxyserver im transparenten Modus funktioniert, sind erweiterte Konfigurationen in den Benutzerprogrammen nicht erforderlich. Die Benutzer werden in diesem Fall gezwungen, den Proxyserver zu verwenden. Legen Sie auf Benutzercomputern die IP-Adresse des Proxyservers (ViPNet Coordinator HW/VA-Knoten) als das Standardgateway fest.

Hinweis. Wenn Sie die Proxyserverparameter konfigurieren, werden die erforderlichen Trafficfilter- und NAT-Regeln automatisch in der Firewall-Konfigurationsdatei (s. Bearbeitungsregeln für offenen Traffic einstellen auf S. 110) angelegt.

Zum Konfigurieren der allgemeinen Proxyserverparameter:

1. Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).
2. Klicken Sie auf der Startseite auf **Proxy-Server**.
3. Klicken Sie im oberen Fensterteil der nächsten Seite wieder auf **Proxy-Server**.
4. Klicken Sie auf der Seite **Proxy-Server** auf die Registerkarte **Allgemeine** und stellen Sie dort die folgenden Parameter ein:
   - Wählen Sie in der Liste **Externer Netzwerkadapter** den Adapter aus, der mit dem Internet verbunden ist.
   - Geben Sie im Feld **Cachegröße** die Cachegröße des Proxyservers an. Der verfügbare Speicherplatz wird neben dem Feld angezeigt.
   - Wenn Sie möchten, dass der Proxyserver im transparenten Modus arbeitet, aktivieren Sie das Kontrollkästchen **„Transparenter" Arbeitsmodus**.

- Klicken Sie auf **Speichern**.

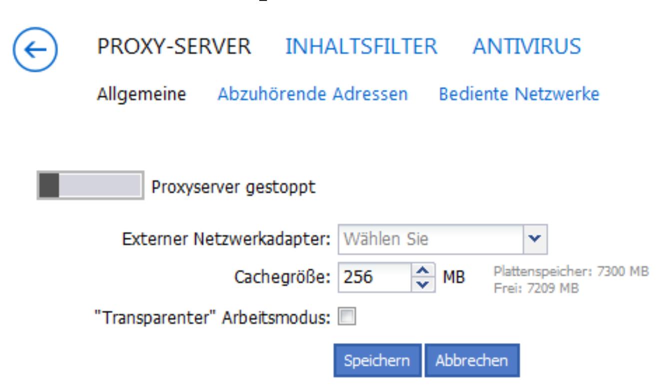


Abbildung 25: Allgemeine Parameter des Proxyservers

5 Legen Sie in der Registerkarte **Abzuhörende Adressen** die IP-Adressen und Ports auf dem Proxyserver fest, die für Benutzeranfragen verwendet werden.

- Zum Hinzufügen einer IP-Adresse und eines Ports zur Liste:
    - Klicken Sie auf **Hinzufügen**.
    - Wählen Sie in der neuen Zeile eine IP-Adresse und geben Sie die Nummer des Ports an, der abgehört werden soll.
    - Klicken Sie auf **Speichern**.

Abbildung 26: Liste der abzuhörenden IP-Adressen

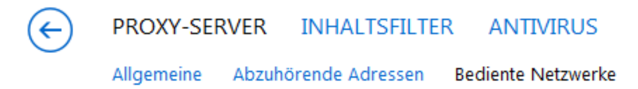
- Zum Ändern einer IP-Adresse oder eines Ports:
    - Doppelklicken Sie auf die Zeile der IP-Adresse, die Sie ändern möchten.
    - Ändern Sie die IP-Adresse oder den **Port**.
    - Klicken Sie auf **Speichern**.
- Zum Löschen einer IP-Adresse oder eines Ports:
    - Klicken Sie in der Zeile der IP-Adresse, die Sie löschen möchten, auf das Symbol ✕ .

- Klicken Sie im Meldungsfenster auf **OK**. Die IP-Adresse und der Port werden gelöscht.

Achtung! Es ist empfehlenswert, Netzwerkadapter mit statischen IP-Adressen als abzuhörende Adapter zu verwenden. Wenn sich die IP-Adressen der Adapter ändern, sollte der Proxyserverdienst gestoppt werden. Dann sollten aktuelle Adapter-IP-Adressen angegeben und der Proxyserver wieder gestartet werden.

6 Definieren Sie in der Registerkarte **Bediente Netzwerke** eine Liste von lokalen Netzwerken, die den Proxyserver verwenden dürfen:

- Zum Hinzufügen der IP-Adresse eines Netzwerks:
  - Klicken Sie auf **Hinzufügen**.
  - Geben Sie in der neuen Zeile die IP-Adresse des Netzwerks in der CIDR-Notation an. Beispiel: 192.168.1.0/24.
  - Drücken Sie die **Eingabe**-Taste.



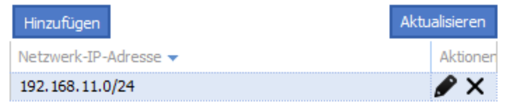


Abbildung 27: Liste von Netzwerken, die den Proxyserver verwenden dürfen

- Zum Ändern der IP-Adresse eines Netzwerks:
  - Klicken Sie auf die IP-Adresse, die Sie ändern möchten.
  - Ändern Sie die Adresse.
  - Drücken Sie die **Eingabe**-Taste.
- Zum Löschen einer IP-Adresse aus der Netzwerkliste:
  - Klicken Sie in der Zeile der IP-Adresse, die Sie löschen möchten, auf das Symbol ✕.
  - Klicken Sie im Meldungsfenster auf **OK**. Die IP-Adresse wird gelöscht.

7 Klicken Sie zum Starten des Proxyservers auf der Registerkarte **Allgemeine** auf den Schalter im oberen Fensterteil. Der Status des Proxyservers wird neben dem Schalter angezeigt.

Hinweis. Bevor Sie den Proxyserver starten, sollten Sie die abzuhörende IP-Adresse und den Port sowie den externen Netzwerkadapter von ViPNet Coordinator HW/VA definieren.

8. Wenn Sie den Internetzugang über den Proxyserver auch für ungeschützte Knoten ermöglichen möchten, sollten Sie zunächst passende Traffic-Verarbeitungsregeln definieren (s. Bearbeitungsregeln für offenen Traffic einstellen auf S. 110).

Inhaltskontrolle konfigurieren

Durch Inhaltskontrolle kann der Zugang zu unerwünschten Webressourcen blockiert werden. Eine URL-Datenbank wird dazu verwendet, den Inhalt von Webressourcen zu filtern. Sie können diese Datenbank im Internet oder von einem anderen ViPNet Coordinator HW/VA-Knoten, der als Server für die URL-Datenbank verwendet wird, abrufen.

Die URLs in der Datenbank können unterschiedlichen Inhaltsklassen zugeordnet werden, zum Beispiel „Glücksspiele“, „Shopping“, „Soziale Netzwerke“, u. s. w. Der Webfilter kann den Zugriff auf Webressourcen dieser Inhaltsklassen (unabhängig voneinander) verhindern. Wenn der Benutzer eine URL anfordert, die dem Muster einer verbotenen URL entspricht, wird die Anforderung abgelehnt und der Benutzer wird darüber informiert, dass die Webseite nicht angezeigt werden kann.

Die Inhaltskontrolle wird automatisch aktiviert, sobald Sie den Proxyserver aktivieren. Zum Einstellen der Inhaltskontrolle-Parameter:

1. Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).
2. Klicken Sie auf der Startseite auf **Proxy-Server**.
3. Klicken Sie im oberen Fensterteil der nächsten Seite auf **Inhaltsfilter**.
4. Öffnen Sie auf der Seite **Inhaltsfilter** die Registerkarte **Allgemeine**. Die Liste der Filterkategorien und die Update-Einstellungen der URL-Datenbank werden angezeigt.

Abbildung 28: Allgemeine Einstellungen der Inhaltsfilter

5 Wenn die Inhaltsfilter zum ersten Mal konfiguriert werden, sollten Sie zunächst eine URL-Datenbank herunterladen.

- Geben Sie die Quelle an, von der Sie die Datenbank herunterladen möchten. Wählen Sie in der Liste **Updatequelle** einen der folgenden Einträge aus:
  - **Internet**: wenn Sie die Datenbankupdates aus dem Internet herunterladen möchten.
  - **Anderes Coordinator HW/VA**: wenn Sie die Datenbankupdates von einem anderen ViPNet Coordinator HW/VA-Knoten, der mit dem aktuell konfigurierten Knoten verbunden ist, herunterladen möchten.
  - Wenn Sie **Anderes Coordinator HW/VA** auswählen, dann wählen Sie in der Liste **Name des Knotens im ViPNet Netzwerk** den Knoten aus, von dem die Datenbankupdates heruntergeladen werden sollen.
- Wenn die URL-Datenbank automatisch aktualisiert werden soll, dann geben Sie in der Liste **Datenbank automatisch aktualisieren** die erforderliche Updatehäufigkeit an. Wenn Sie **nicht aktualisieren** auswählen, wird die automatische Aktualisierung deaktiviert.
- Wenn Sie die URL-Datenbank unverzüglich herunterladen möchten, dann klicken Sie auf **Jetzt aktualisieren**.

6 Wählen Sie die Filterkategorien aus, die vom Inhaltsfilter blockiert werden sollen:

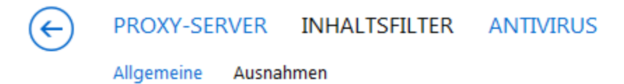
- Wenn bestimmte Kategorien blockiert werden sollen, wählen Sie diese in der Liste **Alle** aus und führen Sie einen der folgenden Schritte durch:
  - ziehen Sie sie mit der Maus in die Liste **Blockierte**;

- klicken Sie auf die Schaltfläche .

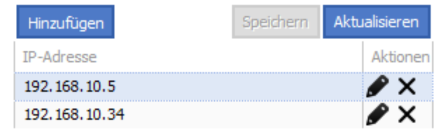
- Wenn bestimmte Kategorien aus der Liste der blockierten Kategorien entfernt werden sollen, wählen Sie diese in der Liste Blockiert aus und führen Sie einen der folgenden Schritte durch:
  - ziehen Sie sie mit der Maus in die Liste **Alle**;
  - klicken Sie auf das Schaltfläche .

7 Klicken Sie auf **Speichern**, um die allgemeinen Einstellungen zu speichern.

8 Wenn nötig, in der Registerkarte **Ausnahmen** konfigurieren Sie eine Liste von Ausnahmen – Knoten, für welche der Webinhalt nicht gefiltert werden soll.



Inhalt von Webseiten mit folgenden IP-Adressen nicht filtern:



IP-Adresse	Aktionen
192.168.10.5	
192.168.10.34	

Abbildung 29: Liste der Inhaltsfilter-Ausnahmen

- Zum Hinzufügen einer IP-Adresse zur Ausnahmenliste:
  - Klicken Sie auf **Hinzufügen**.
  - Geben Sie in der neuen Zeile die Ausnahme-IP-Adresse an.
  - Drücken Sie die **Eingabe**-Taste.
- Zum Ändern einer Ausnahmeadresse:
  - Klicken Sie auf die IP-Adresse, die Sie ändern möchten.
  - Ändern Sie die Adresse.
  - Drücken Sie die **Eingabe**-Taste.
- Zum Löschen einer IP-Adresse aus der Ausnahmenliste:
  - Klicken Sie in der Zeile der IP-Adresse, die Sie löschen möchten, auf das Symbol ✕.
  - Klicken Sie im Meldungsfenster auf **OK**. Die IP-Adresse wird aus der Liste gelöscht.

Antivirus konfigurieren

Wenn Sie ViPNet Coordinator HW/VA als Proxyserver verwenden, dann können Sie eine Antivirus-Überprüfung für den gesamten HTTP-Traffic aktivieren, der den Server in beide Richtungen passiert: aus dem Internet zum Benutzer und vom Benutzer zum Internet (zum Beispiel, wenn der Benutzer einer E-Mail-Nachricht über die Weboberfläche einen Anhang hinzufügt). Die Antivirus-Überprüfung wird vom Programm Clam AntiVirus durchgeführt – es handelt sich um kostenlose Open-Source-Software der Firma Sourcefire.

Gehen Sie wie folgt vor, um den Antivirusschutz zu konfigurieren:

1. Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).
2. Klicken Sie auf der Startseite auf **Proxy-Server**.
3. Klicken Sie im oberen Fensterteil der nächsten Seite auf **Antivirus**.

Abbildung 30: Antivirus-Einstellungen

4. Wenn Antivirus zum ersten Mal konfiguriert wird, sollten Sie zunächst eine Antivirus-Datenbank herunterladen. Klicken Sie dazu auf **Jetzt aktualisieren**.
5. Wenn Sie möchten, dass die Antivirus-Datenbank täglich automatisch aktualisiert wird:
   - Aktivieren Sie das Kontrollkästchen **Datenbank automatisch aktualisieren**.
   - Klicken Sie auf **Speichern**.
6. Klicken Sie auf den Schalter im oberen Fensterteil, um den Antivirusschutz zu aktivieren. Der Status des Antivirus-Moduls wird neben dem Schalter angezeigt.

Konfiguration des VoIP-Servers

Das Appliance ViPNet Coordinator HW/VA besitzt einen eingebauten VoIP-Server, mit dessen Hilfe Sie ein firmeninternes IP-Telefoniesystem einrichten können.

Wenn Sie verschlüsselte Sprachkommunikation zwischen mehreren Firmenniederlassungen gewährleisten möchten, installieren Sie in jeder Niederlassung einen VoIP-Server auf Basis von ViPNet Coordinator HW/VA und bauen Sie Verbindungskanäle (s. Trunk auf S. 246) zwischen diesen Servern auf. Trunks ermöglichen es den Benutzern unterschiedlicher VoIP-Server, sich gegenseitig anzurufen.

Der VoIP-Server unterstützt das SIP-Protokoll, weswegen für Verbindungen zum Server beliebige softwarebasierte SIP-Clients oder SIP-Telefongeräte verwendet werden können. Dabei sollten folgende Bedingungen beachtet werden:

- Softwarebasierte SIP-Clients sollten auf geschützten oder getunnelten Knoten installiert werden. Legen Sie in der SIP-Clientsoftware die sichtbare Adresse von ViPNet Coordinator HW/VA als SIP-Serveradresse fest.
- SIP-Telefongeräte sollten vom ViPNet Coordinator HW/VA-Knoten getunnelt werden. Legen Sie die IP-Adresse des externen Adapters von ViPNet Coordinator HW/VA als SIP-Serveradresse fest.
- Damit der reibungslose Betrieb von SIP-Clients, die vom ViPNet Coordinator HW/VA getunnelt werden, sichergestellt werden kann, konfigurieren Sie Filterregeln für den offenen Traffic (s. Regeln zur Filterung des Traffics auf S. 112), die eingehende lokale Verbindungen getunnelter Clients zum ViPNet Coordinator HW/VA über TCP und UDP unter Verwendung von Port 5060 erlauben.
- Wenn Sie mobile Geräte über einen IPsec-Kanal mit ViPNet Coordinator HW/VA verbinden möchten (s. Bereitstellung eines sicheren Zugangs zum Firmen-LAN von mobilen Geräten über IPsec-Kanäle auf S. 152), dann konfigurieren Sie im ViPNet Network Manager den ViPNet Coordinator HW/VA–Knoten, der diese mobilen Geräte tunneln soll. Wählen Sie dazu den ViPNet Coordinator HW/VA-Knoten aus und legen auf der Registerkarte **Tunnelung** den IP-Adressbereich fest, der für zu tunnelende IPsec-Geräte verwendet werden soll. Dieser Bereich beträgt 192.168.30.1 — 192.168.30.40.

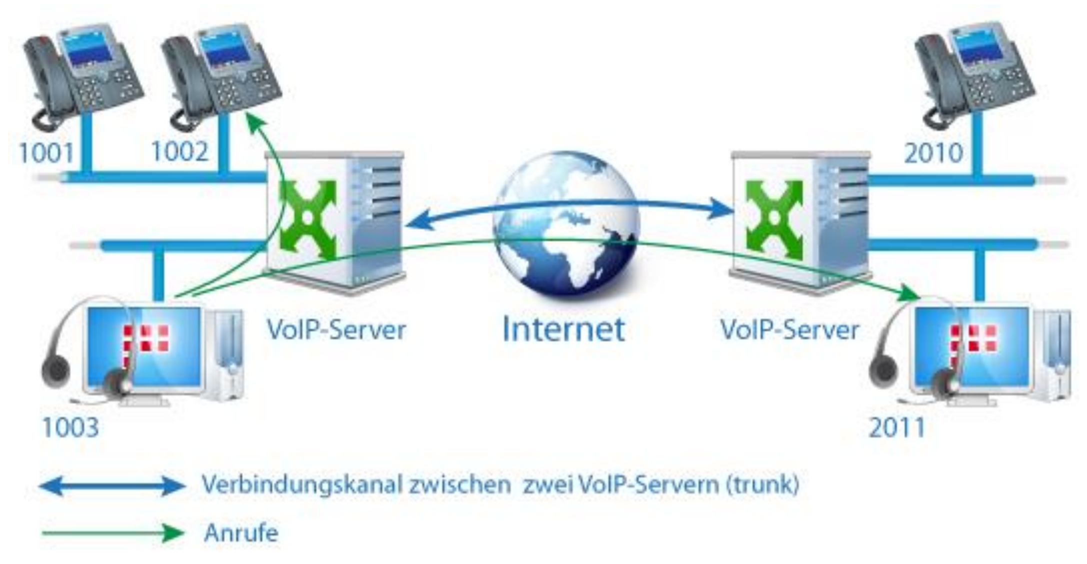


Abbildung 31: Verwendung des integrierten VoIP-Servers

Konfiguration der allgemeinen VoIP-Server-Einstellungen

Gehen Sie wie folgt vor, um den integrierten VoIP-Server zu (de-)aktivieren und die allgemeinen Servereinstellungen zu konfigurieren:

1. Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).
2. Klicken Sie auf der Startseite auf **VoIP-Server**.
3. Klicken Sie im oberen Fensterteil der nächsten Seite auf **Allgemeine**.

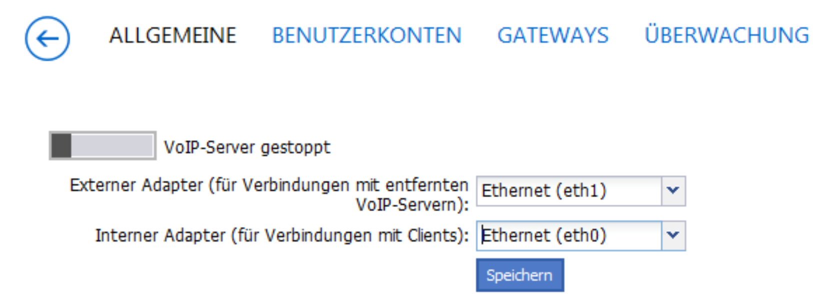


Abbildung 32: Allgemeine VoIP-Servereinstellungen

4. Wählen Sie in der Liste **Externer Adapter** den Netzwerkadapter auf dem ViPNet Coordinator HW/VA aus, über welchen Verbindungen zu entfernten VoIP-Servern hergestellt werden sollen (s. Konfiguration von VoIP-Trunks auf S. 101).

5 Wählen Sie in der Liste **Interner Adapter** den Netzwerkadapter aus, der von Ihren VoIP-Clients für den Verbindungsaufbau zum Server verwendet werden soll.

6 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

7 Klicken Sie auf den Schalter im oberen Fensterteil, um den VoIP-Server zu starten. Der Status des VoIP-Servers wird neben dem Schalter angezeigt.

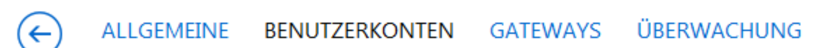
Verwaltung der Benutzerkonten

Zum Verwalten der Benutzerkonten, die auf Ihrem VoIP-Server registriert sind:

1 Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).

2 Klicken Sie auf der Startseite auf **VoIP-Server**.

3 Klicken Sie im oberen Fensterteil der nächsten Seite auf **Benutzerkonten**. Es wird eine Liste der Benutzerkonten angezeigt.



Benutzerkonten, die auf dem VoIP-Server registriert sind:

Hinzufügen | Aktualisieren

Telefonnummer	Name	Nachname	Passwort	Aktionen
3450	John	Smith	dfsdfsdf	✎ ✕
3451	Eric	Cartman	sdfsdf	✎ ✕

Abbildung 33: Liste der Benutzerkonten

4 Zum Hinzufügen eines neuen VoIP-Benutzerkontos:

- Klicken Sie auf **Hinzufügen**.
- Definieren Sie in der neuen Zeile eine 4-stellige Telefonnummer ein, geben Sie den Namen des Benutzers und ein Passwort für das Benutzerkonto ein.
- Klicken Sie auf **Speichern**.

5 Zum Ändern eines Benutzerkontos:

- Doppelklicken Sie auf die Zeile des Benutzerkontos, das Sie ändern möchten.
- Ändern Sie die Kontoeigenschaften.
- Klicken Sie auf **Speichern**.

6 Zum Löschen eines Benutzerkontos:

6.1 Klicken Sie in der Zeile des Kontos, das Sie löschen möchten, auf das Symbol ✕.

6.2 Klicken Sie im Meldungsfenster auf **OK**. Das Benutzerkonto wird gelöscht.

7 Die Telefonnummern der Benutzer, die zum gegebenen Zeitpunkt mit dem Server verbunden sind, werden als aktiv markiert. Wenn Sie Detailinformationen zu einem aktiven Benutzer anzeigen möchten, klicken Sie auf die Telefonnummer des Benutzers.

Call-ID	Yjc3OTJkM2ZiYWRiY2RmYTY3YmFlMWQ3MTJjMr
User	5423@127.0.0.1
Contact	"vasily"
Agent	3CXPhone 6.0.26523.0
Status	Registered(UDP)(unknown) EXP(2013-04-04 13 EXPSECS(178)
IP	192.168.13.247
Port	2112
Auth-User	5423

Abbildung 34: Detaillierte Benutzerinformationen

Konfiguration von VoIP-Trunks

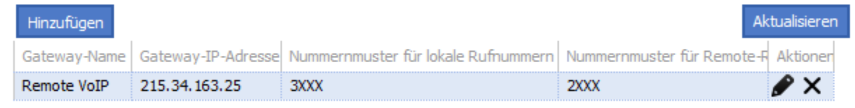
Wenn Sie mit Benutzern von Remotenetzwerken über VoIP kommunizieren möchten, können Sie VoIP-Trunks konfigurieren, die den integrierten VoIP-Server auf Ihrem ViPNet Coordinator HW/VA-Knoten mit den entfernten VoIP-Servern verbinden (s. Abbildung auf S. 99).

Zum Verwalten der VoIP-Trunks:

1 Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an (s. Anmeldung an der Webschnittstelle auf S. 48).

2 Klicken Sie auf der Startseite auf **VoIP-Server**.

3 Klicken Sie im oberen Fensterteil der nächsten Seite auf **Gateways**. Es wird eine Liste von VoIP-Trunks angezeigt.



Verbindung mit entfernten VoIP-Servern herstellen:

Hinzufügen | Aktualisieren

Gateway-Name	Gateway-IP-Adresse	Nummernmuster für lokale Rufnummern	Nummernmuster für Remote-R	Aktionen
Remote VoIP	215.34.163.25	3XXX	2XXX	

Abbildung 35: Liste der Trunks

4 Zum Hinzufügen eines neuen VoIP-Trunks:

4.1 Klicken Sie auf **Hinzufügen**.

4.2 Definieren Sie in der neuen Zeile die Eigenschaften des neuen Trunks:

- Geben Sie in der Spalte **Gateway-Name** einen eindeutigen Namen für den neuen Trunk an.
- Geben Sie in der Spalte **Gateway-IP-Adresse** die IP-Adresse des entfernten VoIP-Servers an.
- Definieren Sie in der Spalte **Nummermuster für lokale Rufnummern** das Rufnummernmuster für die lokalen Telefonnummern, die mit Remote-Nummern kommunizieren sollen. Das Muster sollte die erste Ziffer einer lokalen Nummer gefolgt von `xxx`-Symbolen enthalten, zum Beispiel `3xxx`.
- Definieren Sie in der Spalte **Nummermuster für Remote-Rufnummern** das Rufnummernmuster für die Remote-Telefonnummern, die mit Ihren lokalen Nummern kommunizieren sollen. Beispiel: `2xxx`.

4.3 Klicken Sie auf **Speichern**.

5 Zum Ändern eines VoIP-Trunks:

5.1 Doppelklicken Sie auf die Zeile des Trunks, den Sie ändern möchten.

5.2 Ändern Sie die Trunk-Eigenschaften.

5.3 Klicken Sie auf **Speichern**.

6 Zum Löschen eines VoIP-Trunks:

6.1 Klicken Sie in der Zeile des Trunks, den Sie löschen möchten, auf das Symbol ✕.

6.2 Klicken Sie im Meldungsfenster auf **OK**. Der Trunk wird gelöscht.

Konfiguration des IPsec-Gateways

In Unternehmensnetzwerken ist es oft erforderlich, die Verbindungen zu Remotenetzwerken oder -Knoten zu schützen. Beispiel: im Unternehmensnetzwerk ist ein Anwendungsserver installiert, der über einen abgesicherten Kanal aus dem Internet zugänglich sein soll. Diese Aufgabe kann nicht immer mit Hilfe der ViPNet Technologie gelöst werden. Es ist zum Beispiel nicht möglich, ViPNet Software auf mobile Geräte zu installieren.

Bei Verwendung von ViPNet Coordinator HW/VA kann der Traffic mittels Verschlüsselung über das IPsec-Protokoll geschützt werden. In diesem Fall tritt ViPNet Coordinator HW/VA als ein ViPNet IPsec-Gateway auf. ViPNet Coordinator HW/VA unterstützt zwei Typen von IPsec-Verbindungen: Site-to-Site (s. Verbindungen über einen geschützten IPsec-Kanal auf S. 161) und Client-to-Site (s. Bereitstellung eines sicheren Zugangs zum Firmen-LAN von mobilen Geräten über IPsec-Kanäle auf S. 152). In beiden Fällen unterstützt ViPNet Coordinator HW/VA die Authentifizierung über Pre-Shared Key (PSK) oder über ein Zertifikat (RSA). ViPNet Coordinator HW/VA unterstützt bis zu 40 gleichzeitige Client-to-Site IPsec-Verbindungen.

Achtung! Wenn Sie einen ViPNet Coordinator HW/VA als IPsec-Gateway verwenden, dann sollte eine öffentliche statische IP-Adresse zur Verfügung stehen. Deswegen kann ein ViPNet Coordinator HW/VA nicht als IPsec-Gateway bereitgestellt werden, wenn er sich hinter einer NAT befindet.

Wählen Sie in Abhängigkeit von der Art der Authentifizierung die Vorgehensweise aus, die für Sie beim Konfiguration des Dienstes auf dem ViPNet Coordinator HW/VA-Knoten am einfachsten ist:

- Wenn Sie PSK-Authentifizierung verwenden möchten, dann ist es einfacher, die IPsec-Verbindung in ViPNet Network Manager zu konfigurieren.

  Wählen Sie zum Konfigurieren der IPsec-Verbindung in ViPNet Network Manager in der Knotenliste den benötigten Knoten aus und konfigurieren Sie dann in der Registerkarte **IPsec-Verbindung** die erforderlichen Einstellungen. Nachdem die Schlüssel von ViPNet Network Manager versendet und auf dem Knoten angewendet wurden, treten diese Einstellungen ebenfalls in Kraft. Weitere Informationen über die Arbeit mit ViPNet Network Manager und den Versand der Schlüssel s. Dokument „ViPNet VPN. Benutzerhandbuch“.

- Wenn Sie RSA-Authentifizierung verwenden möchten, dann konfigurieren Sie diese mit Hilfe der Befehlszeilenschnittstelle. Die Konfiguration der RSA-Authentifizierung kann im ViPNet Network Manager oder durch Web-Schnittstelle nicht durchgeführt werden.

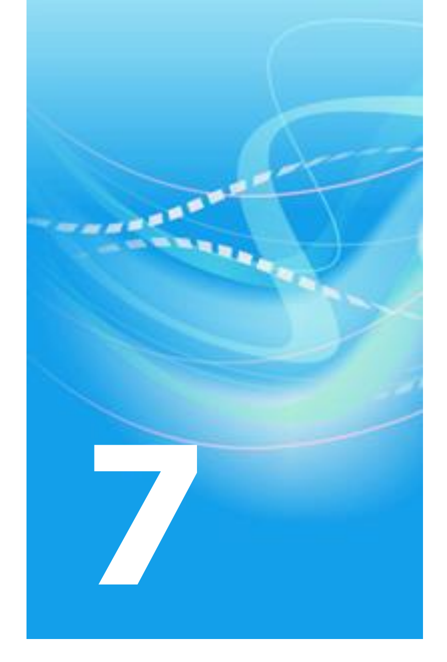
Achtung! Wenn Sie eine IPsec-Verbindung vom Typ Client-to-Site oder Site-to-Site mit Hilfe der Befehlszeile konfigurieren, dann sollten Sie die zugehörigen IPsec-Einstellungen für den ViPNet Coordinator HW/VA-Knoten auf keinen Fall in ViPNet Network Manager nachträglich ändern. Anderenfalls gehen alle Einstellungen, die Sie über die Befehlszeilenschnittstelle vorgenommen haben, nach dem Senden der Schlüssel an den ViPNet Coordinator HW/VA-Knoten verloren. Sie können jedoch eine Site-to-Site Verbindung in ViPNet Network Manager und eine Client-to-Site Verbindung über die Befehlszeile konfigurieren (und umgekehrt).

Damit sichergestellt wird, dass die Einstellungen später nicht zufällig geändert werden, deaktivieren Sie im Hauptfenster von ViPNet Network Manager in der Panel-Ansicht auf der Registerkarte **IPsec-Verbindung** das folgende Kontrollkästchen:

  - Wenn Sie eine Verbindung vom Typ Site-to-Site über die Befehlszeile konfigurieren, dann deaktivieren Sie das Kontrollkästchen **Coordinator für geschützte IPsec-Verbindung mit anderen Netzwerken verwenden**.
  - Wenn Sie eine Verbindung vom Typ Client-to-Site über die Befehlszeile konfigurieren, dann deaktivieren Sie das Kontrollkästchen **Coordinator als IPsec-Gateway für Anbindung von Smartphone-Clients verwenden**.

Weitere Informationen über die Konfiguration von IPsec-Verbindungen auf einem ViPNet Coordinator HW/VA-Knoten mit Hilfe der Befehlszeilenschnittstelle finden Sie in den folgenden Abschnitten:

- Konfiguration einer Site-to-Site Verbindung s. Verbindungen über einen geschützten IPsec-Kanal (auf S. 161).
- Konfiguration einer Client-to-Site Verbindung s. Bereitstellung eines sicheren Zugangs zum Firmen-LAN von mobilen Geräten über IPsec-Kanäle (auf S. 152).



Konfiguration der integrierten Firewall

Über eine integrierte Firewall

Der ViPNet Coordinator HW/VA-Knoten verfügt als Coordinator über eine integrierte Firewall, um den weitergeleiteten IP-Traffic zu verarbeiten:

- Filterung der IP-Pakete gemäß den Parametern des Pakets (wie Quell- oder Zieladresse, Adapter, Port, u. s. w.). Separate Filterregeln können für die folgenden Traffictypen konfiguriert werden:
  - Verschlüsselter Traffic zwischen ViPNet Knoten, der über den Coordinator geleitet wird.
  - Getunnelter Traffic (Traffic von Knoten, die vom Coordinator getunnelt werden).
  - Nicht verschlüsselter Traffic, der von einem ungeschützten Knoten (Knoten ohne installierte ViPNet Software) ausgeht.
  - Über den Coordinator weitergeleiteter Traffic (z. B. beim Zugriff eines Knotens im lokalen LAN auf das Internet, wobei der Coordinator als Standardgateway verwendet wird).

  Standardmäßig wird der Traffic, der zwischen ViPNet Knoten oder zwischen getunnelten Knoten ausgetauscht wird, von der Firewall durchgelassen. Jeder ViPNet Knoten kann den IP-Traffic mit folgenden Knoten austauschen:
  - andere ViPNet Knoten, die mit dem betroffenen Knoten im VPN verbunden sind;
  - Knoten, die von Coordinatoren getunnelt werden, die mit dem betroffenen Knoten im VPN verbunden sind.

  Standardmäßig wird der weitergeleitete und der eintreffende nicht verschlüsselte Traffic auf dem Coordinator blockiert. Sie können den Traffic erlauben, indem Sie die Sicherheitsstufe ändern und die Trafficverarbeitungsregeln auf den Adaptern des Coordinators konfigurieren.

Tipp. Wenn z. B. der Zugriff eines ungeschützten Knotens im LAN auf einen ViPNet Coordinator HW/VA-Knoten über die Webschnittstelle (s. Verwalten von ViPNet Coordinator HW/VA-Knoten auf S. 46) ermöglicht werden soll, dann sollte der eingehende nicht verschlüsselte Traffic, der von der IP-Adresse des ungeschützten Knotens ausgeht und an den ViPNet Coordinator HW/VA-Knoten adressiert ist, auf dem entsprechenden Netzwerkadapter explizit erlaubt werden.

- NAT für nicht verschlüsselten Traffic.

- Antispoofing, eine Technologie zur Blockierung von IP-Paketen mit gefälschten Quelladressen.

  Bei allen IP-Paketen, die auf einem Netzwerkadapter des Coordinators eintreffen, wird eine Quell-IP-Adresse erwartet, die zu einem bestimmten Adressbereich gehört. Beispiel: auf einem Adapter, der mit dem LAN verbunden ist, sollten keine IP-Pakete eintreffen, die eine öffentliche Quelladresse besitzen.

  Die Antispoofing-Technologie verwendet eine Reihe von formalisierten Regeln, die Quell-IP-Adressen beschreiben, die am jeweiligen Netzwerkadapter zu erwarten sind. Alle IP-Pakete, die diesen Regeln nicht entsprechen, werden blockiert.

  Weitere Details zur Verwendung und Konfiguration von Antispoofing s. Dokument „ViPNet Coordinator HW/VA. Referenzhandbuch“.

Änderung der Sicherheitsstufe auf einem Netzwerkadaper

Die Sicherheitsstufe (s. Sicherheitsstufen auf S. 26) bestimmt die Richtlinien für die Filterung des offenen Traffics, der den Netzwerkadapter passiert. Für jeden Netzwerkadapter existiert eine eigene Konfigurationsdatei, in welcher die Sicherheitsstufe mit Hilfe des Parameters `mode` definiert werden kann.

Hinweis. Standardmäßig ist auf allen Netzwerkadaptern von ViPNet Coordinator HW/VA die zweite Sicherheitsstufe eingestellt. Es wird empfohlen, die vierte Sicherheitsstufe zeitlich eingeschränkt ausschließlich für Testzwecke zu verwenden.

Wenn die Sicherheitsstufe auf irgendeinem Netzwerkadapter geändert werden soll, dann führen Sie die nachfolgenden Schritte aus:

1. Wechseln Sie im Kommandointerpreter in den Administratormodus mit Hilfe des Befehls `enable`.
2. Stoppen Sie mit Hilfe des Befehls `iplir stop` den ViPNet Treiber.
3. Führen Sie den folgenden Befehl aus, um die Konfigurationsdatei des Netzwerkadapters zu editieren:

```
iplir config <Adaptername>
```

Hinweis. Benutzen Sie den Befehl `inet show interface`, um eine Liste aller Netzwerkadapter anzuzeigen.

4. Geben Sie als Wert für den Parameter mode die Nummer der benötigten Sicherheitsstufe an:

1 – Alle Verbindungen blockieren.

2 – Nur erlaubte Verbindungen durchlassen.

3 – Ausgehende Verbindungen erlauben außer verbotene.

4 – Alle Verbindungen erlauben.

5 Drücken Sie die Tastenkombination **Strg+O**, um die Konfigurationsdatei zu speichern, und drücken Sie dann die **Eingabe**.

6 Drücken Sie die Tastenkombination **Strg+X**, um die Datei zu schließen.

7 Starten Sie den ViPNet Treiber mit Hilfe des Befehls `iplir start`.

Bearbeitungsregeln für offenen Traffic einstellen

ViPNet Coordinator HW/VA kann die IP-Adressen für den nicht verschlüsselten (offenen) IP-Traffic filtern und übersetzen. Die Verarbeitungsregeln für nicht verschlüsselte IP-Pakete sind in der Firewall-Konfigurationsdatei enthalten. Bearbeiten Sie die Firewall-Konfigurationsdatei unter Verwendung der Befehlszeilenschnittstelle, um die Regeln zu konfigurieren.

Zum Bearbeiten der Konfigurationsdatei der Firewall sollte der Befehl `iplir config firewall` ausgeführt werden.

Die Konfigurationsdatei der Firewall besteht aus mehreren Bereichen. Die Verarbeitungsregeln für den offenen Traffic sind in den folgenden Bereichen enthalten:

- `[local]` enthält Filterregeln für lokale IP-Pakete. Das sind Pakete, deren Sender oder Empfänger ein Netzwerkknoten mit installiertem ViPNet Coordinator HW/VA ist.
- `[broadcast]` enthält Filterregeln für Broadcast-IP-Pakete.
- `[forward]` enthält Filterregeln für Transit-IP-Pakete. Das sind Pakete, die den Netzwerkknoten mit darauf installierter ViPNet Coordinator HW/VA-Software auf ihrem Weg vom Sender zum Empfänger passieren. Der aktuelle Netzwerkknoten tritt weder als Absender noch als Empfänger der Transit-IP-Pakete auf.
- `[tunnel]` enthält Filterregeln für die IP-Pakete der getunnelten Knoten. Oder anders ausgedrückt: es handelt sich um Pakete, die zwischen den vom ViPNet Coordinator HW/VA getunnelten Knoten und den ViPNet Knoten oder anderen Knoten, die von ViPNet Coordinatoren getunnelt sind, ausgetauscht werden.
- `[nat]` enthält Regel der Adressenübersetzung. ViPNet Coordinator HW/VA unterstützt zwei Typen der Adressenübersetzung:
  - Übersetzung der Absenderadresse, die auch als dynamisches NAT bezeichnet wird. Dieser Typ der Adressumsetzung wird verwendet, wenn der Internetzugang für Computer eingerichtet werden soll, die über private IP-Adressen verfügen. In diesem Fall wird in IP-Paketen, die vom Computer des lokalen Netzwerks an das externe Netzwerk weitergeleitet werden, die Absenderadresse von ViPNet Coordinator HW/VA durch die eigene externe IP-Adresse ersetzt. In Antwort-IP-Paketen wird die Empfängeradresse (externe IP-Adresse des Computers mit installiertem ViPNet Coordinator HW/VA) durch die private IP-Adresse des Rechners im lokalen Netzwerk ersetzt.

- Übersetzung der Empfängeradresse, die auch als statisches NAT bezeichnet wird. Dieser Typ der Adressumsetzung wird verwendet, wenn Zugang aus dem Internet zu Computern im lokalen Netzwerk ermöglicht werden soll. In diesem Fall wird in IP-Paketen, die auf einem bestimmten Port der externen IP-Adresse von ViPNet Coordinator HW/VA eintreffen, die Empfängeradresse durch die angegebene IP-Adresse des lokalen Netzwerks ersetzt. In Antwort-IP-Paketen wird die Absenderadresse ersetzt.

Jeder der aufgezählten Bereiche kann eine oder mehrere Bearbeitungsregeln für offene IP-Pakete enthalten. Jede Regel wird durch den Parameter rule beschrieben. Der Wert dieses Parameters setzt sich aus den folgenden Bestandteilen zusammen:

```
rule= <Steuerkomponente> <Aktion> <Bedingung>
```

Hinweis. Für die Filterregel des Traffics kann auch ein Zeitplaner definiert werden. In diesem Dokument wird die Konfiguration des Zeitplaners nicht behandelt.

Jede Komponente der Regel kann aus mehreren Parametern (Lexemen) bestehen.

Die Steuerkomponente beschreibt Eigenschaften der Regel, die sich nicht unmittelbar auf die Bearbeitung der Pakete beziehen, und wird immer am Anfang der Regel aufgeführt. Die Bedingung definiert Parameter von Paketen, für welche die Regel angewendet werden soll. In Bezug auf Pakete, die die Regelbedingung erfüllen, wird die angegebene Aktion durchgeführt.

Die Steuerkomponente bleibt bei allen Bearbeitungsregeln des IP-Traffics gleich, während sich Aktionen und Bedingungen für Filterregeln (s. Regeln zur Filterung des Traffics auf S. 112) und Regeln der Adressenübersetzung (auf S. 114) ändern können

Die Steuerkomponente kann folgende optionale Parameter beinhalten:

- `num <Nummer>`: Parameter, der die Priorität der Regel innerhalb des Bereichs bestimmt. Die Nummer kann einen Wert zwischen 0 und 65535 annehmen.

  Regeln werden in Bezug auf IP-Pakete in Übereinstimmung mit ihrer Priorität angewendet. Wenn keine Nummer angegeben wird, wird die Priorität der Regel ausgehend von der Reihenfolge der Regeln innerhalb des Bereichs automatisch festgelegt.

- `disable`: Parameter, der für zeitweise Deaktivierung der Regel verwendet wird. Wenn der Parameter `disable` fehlt, bedeutet das, dass die Regel aktiv ist.

Die Konfiguration von Aktionen und Bedingungen für Regeln der Traffic-Filterung und Adressenübersetzung wird in den entsprechenden Abschnitten behandelt.

Wenn Sie einen IP-Adressbereich definieren, dann können Sie dazu das Composite Range-Token `internet` verwenden, das den Bereich `anyip` mit Ausnahme der drei privaten IP-Adressbereiche repräsentiert:

- `10.0.0.0-10.255.255.255`
- `17.16.0.0-172.31.255.255`
- `192.168.0.0-192.168.255.255`

Regeln zur Filterung des Traffics

Filterregeln für offene (nicht verschlüsselte) IP-Pakete werden in den Bereichen `[local]`, `[broadcast]`, `[tunnel]` und `[forward]` der Firewall-Konfigurationsdatei definiert.

Standardmäßig sind folgende Regeln definiert:

- In den Bereichen `[local]` und `[broadcast]` eine Reihe von Regeln, die den Durchlass von IP-Paketen, die von DHCP-, NetBIOS-, DNS- und NTP-Diensten verwendet werden, gewährleistet.
- Im Bereich `[tunnel]` eine Regel, die Verbindungen zwischen allen getunnelten Knoten von ViPNet Coordinator HW/VA und allen geschützten Knoten, mit denen der ViPNet Coordinator HW/VA-Knoten verbunden ist, erlaubt. In den meisten Fällen ist das Einstellen zusätzlicher Regeln in diesem Bereich nicht erforderlich.

Jede Regel wird durch den Parameter rule beschrieben. Der Wert dieses Parameters setzt sich aus den folgenden Bestandteilen zusammen:

```
rule= <Steuerkomponente> <Aktion> <Bedingung>
```

Eine Beschreibung der Steuerkomponente ist im Abschnitt Bearbeitungsregeln für offenen Traffic einstellen (auf S. 110) aufgeführt.

Die Aktion bestimmt, was mit dem IP-Paket, dessen Parameter die Regelbedingung (s. weiter unten) erfüllen, geschehen soll. Die Aktion wird durch einen der zwei Parameter festgelegt:

- `pass` – IP-Paket durchlassen.
- `drop` – IP-Paket blockieren.

Die Bedingung definiert Parameter von Paketen, für welche die Regel angewendet werden soll. Die Bedingung wird mit Hilfe folgender Parameter festgelegt:

- `proto <Protokoll>` – obligatorischer Parameter, der das Protokoll der Netzwerkschicht, zu welchem das IP-Paket gehören soll, festlegt. Als Protokoll können folgende Werte angegeben werden:
  - `tcp`, `udp` oder `icmp`.
  - Nummer beliebiger IP-Protokolle.
  - `any` – alle Protokolle.

  Wenn von einer Regel Pakete unterschiedlicher Protokolle bearbeitet werden sollen, dann können die Protokolle durch Komma getrennt aufgelistet werden.

Hinweis. Für Regeln im Bereich `[broadcast]` können ausschließlich die Werte udp und icmp angegeben werden.

- `from <Adressliste>` — obligatorischer Parameter, der die IP-Adresse und den Port des Paketabsenders festlegt. Adresse und Port sollten durch einen Doppelpunkt getrennt aufgeführt werden, zum Beispiel: `192.168.201.1:22`. Wenn kein Port angegeben wird, gilt die Bedingung für alle Ports.

Hinweis. Es dürfen keine Portnummern angegeben werden, falls als Protokoll `icmp` oder `any` definiert wurde.

Neben einzelnen IP-Adressen und Ports können auch Adress- oder Portbereiche oder IP-Adressmasken definiert werden. Es können auch mehrere IP-Adressen durch Komma getrennt angegeben werden. Zum Beispiel:

- `192.168.1.1-192.168.1.10:22`
- `192.168.201.0/24:1024-65535`
- `192.168.1.1-192.168.1.10:22,172.16.1.0.24:25`

Statt Adressen oder Adressbereichen können auch folgende Schlüsselwörter angegeben werden:

- `anyip` – alle Adressen (Bereich 0.0.0.0–255.255.255.255).
- `broadcast` – die Adresse 255.255.255.255.

- `to <Adressliste>` – obligatorischer Parameter, der die IP-Adresse und den Port des Paketempfängers definiert. Die Adressen und Ports werden genauso definiert wie beim Parameter from.

  Im Bereich `[broadcast]` können für den Parameter to ausschließlich folgende IP-Adressen angegeben werden:

  - `broadcast` – repräsentiert die Adresse 255.255.255.255.
  - `directed-broadcast` – repräsenteirt Broadcast-Adressen aller Subnetze, die an die Netzwerkadapter des Computers angeschlossen sind.
  - Konkrete Broadcast-Adressen von Subnetzen, die an die Netzwerkadapter des Computers angeschlossen sind.

- `in` oder `out` – optionaler Parameter, der die Verbindungsrichtung (eingehende oder ausgehende Verbindung) angibt. Beim Festlegen dieser Parameter sollte darauf geachtet werden, dass die Verbindungsrichtung und die Senderichtung bestimmter IP-Pakete nicht miteinander verwechselt werden.

  Die Festlegung der Verbindungsrichtung ist optional. Es wird dabei angenommen, dass Verbindungen, die in beiden Richtungen aufgebaut werden, unter die Bedingung fallen.

  Für das TCP-Protokoll werden Verbindungen immer überwacht. In manchen Fällen kann die Verbindungsrichtung auch für das UDP-Protokoll ermittelt werden.

Hinweis. Für Regeln im Bereich `[forward]` und `[tunnel]` kann keine Verbindungsrichtung festgelegt werden.

Beispiele für Filterregeln für IP-Pakete:

```
rule= num 15 pass proto any from anyip to 192.168.201.1:22 in

rule= pass proto tcp,udp from anyip:53 to 192.168.0.0/16,172.16.1.0/24
```

Regeln der Adressenübersetzung

Die Regeln der Adressenübersetzung (NAT) für offene (nicht verschlüsselte) IP-Pakete werden im Bereich `[nat]` der Firewall-Konfigurationsdatei definiert.

Jede Regel der Adressenübersetzung wird durch den Parameter rule beschrieben, dessen Wert sich aus folgenden Komponenten zusammensetzt:

```
rule= <Steuerkomponente> <Aktion> <Bedingung>
```

Eine Beschreibung der **Steuerkomponente** ist im Abschnitt Bearbeitungsregeln für offenen Traffic einstellen (auf S. 110) aufgeführt.

Aktion wird durch `change` deklariert mit den Angaben, was und wodurch ersetzt wird. Je nachdem, ob es sich um eine dynamische oder statische Umsetzung handelt, haben die Regeln folgende Schreibweise:

- Bei der dynamischen Umsetzung: `change src=<Adresse>:dynamic`

  `<Adresse>` – ist die IP-Adresse des externen Netzwerkadapters des ViPNet Coordinator HW/VA. Zum Beispiel: `change src=194.87.0.8:dynamic`.

- Bei der statischen Umsetzung: `change dst=<Adresse>:<Port>`

  `<Adresse>` und `<Port>` sind die IP-Adresse und der Port des Netzwerkknotens im lokalen Netzwerk. Zum Beispiel: `change dst=192.168.201.1:8080`.

Bedingung die NAT-Regel hat die gleiche Schreibweise wie die Bedingung der Filterregel, allerdings mit einigen Abweichungen:

- Beim dynamischen NAT für `proto` und `to` muss `anyip` angegeben werden.
- Beim dynamischen NAT definiert `from` die IP-Adressen des geschützten Netzwerks, welche umgesetzt werden sollen. Dabei können in `from` nur einzelne oder mehrere gelistete IP-Adressen, IP-Adressen Bereiche und Masken angegeben werden. Es können keine Ports oder Portbereiche definiert werden.
- Beim statischen NAT soll `from` auf `anyip` gesetzt werden und bei `to` sollen die externe IP-Adresse und der Port des ViPNet Coordinator HW/VA angegeben werden, auf die die IP-Pakete eingehen, welche der Umsetzung unterliegen. In diesem Fall für `to` können nur einzelne oder mehrere gelistete IP-Adressen und Ports angegeben werden. Keine Adressen- Masken- und Portbereiche sind zugelassen.

Beispiele für NAT-Regeln:

- Dynamische Umsetzung:

```
rule= num 10 change src=194.87.0.8:dynamic proto any from 192.168.201.0/24
to anyip
```

- Statische Umsetzung:

```
rule= num 100 change dst=10.0.0.7:8080 proto tcp from anyip to
194.87.0.8:80
```

Logdatei der IP-Pakete

Die Logdatei der registrierten IP-Pakete enthält Daten über verschlüsselte und nicht verschlüsselte IP-Pakete, die vom ViPNet Treiber des ViPNet Coordinator HW/VAs verarbeitet wurden. Diese Daten werden für alle Netzwerkadapter des Computers gesammelt. Sie können die Protokollierungseinstellungen für jeden Netzwerkadapter separat konfigurieren (s. Konfiguration der Logdatei der IP-Pakete auf S. 116).

Wenn nötig, können Sie nach Einträgen in der Logdatei der IP-Pakete suchen, indem Sie unterschiedliche IP-Paketparameter als Suchparameter verwenden (s. Logdatei registrierter IP-Pakete anzeigen auf S. 117).

Konfiguration der Logdatei der IP-Pakete

Daten über Ereignisse, die in Zusammenhang mit der Verarbeitung von IP-Paketen durch ViPNet Coordinator HW/VA-Netzwerkadapter stehen, werden in der Registrierungslogdatei erfasst (s. Logdatei registrierter IP-Pakete anzeigen auf S. 117). Für jeden Netzwerkadapter können das Ausmaß der Detalisierung der registrierten Daten und die maximale Größe der Logdatei festgelegt werden.

Führen Sie die folgenden Schritte aus, um die Parameter der Registrierung von IP-Paketen, die einen bestimmten Netzwerkadapter passieren, zu konfigurieren:

1 Wechseln Sie in der Befehlszeilenschnittstelle in den Administratormodus mit Hilfe des Befehls `enable`.

2 Führen Sie den folgenden Befehl aus, um die Konfigurationsdatei des Netzwerkadapters zu editieren:

```
iplir config <Adaptername>
```

Hinweis. Benutzen Sie den Befehl `inet show interface`, um eine Liste aller Netzwerkadapter anzuzeigen.

3 Geben Sie im Bereich `[db]` die benötigten Werte für die folgenden Parameter an:

- `maxsize`: maximale Größe der Logdatei in MB.

  Wenn die Größe der Logdatei den angegebenen maximal Wert erreicht, beginnt das System, die ältesten Einträge durch neue zu ersetzen.

Wenn der Wert dieses Parameters gleich Null ist, dann wird für den betroffenen Netzwerkadapter keine Logdatei geführt.

- `timediff`: Zeitintervall (in Sekunden), innerhalb von welchem Ereignisse mit gleichen Merkmalen in einem Eintrag der Logdatei zusammengefasst werden. Vorgegebener Standardwert ist 60 Sekunden.

  Beispiel: Einträge über durchgelassene verschlüsselte IP-Pakete, bei denen die Adressen und Ports des Absenders und de s Empfängers übereinstimmen, werden zusammengefasst.

  Wenn der Wert dieses Parameters gleich Null ist, dann wird jedes IP-Paket mit einem eigenen Eintrag der Logdatei registriert.

- `registerall`: Parameter, der die Registrierung aller IP-Pakete aktiviert oder deaktiviert. Dieser Parameter kann die folgenden Werte annehmen:
  - `on`: alle IP-Pakete registrieren;
  - `off` (Standardwert): nur blockierte IP-Pakete sowie Ereignisse, die in Zusammenhang mit Änderungen von IP-Adressen der ViPNet Netzwerkknoten stehen, registrieren;
- `registerbroadcast`: Parameter, der die Registrierung von Broadcast-IP-Paketen aktiviert oder deaktiviert. Dieser Parameter kann die folgenden Werte annehmen:
  - `on`: Broadcast-Pakete registrieren,
  - `off` (Standardwert): Broadcast-Pakete nicht registrieren.
- `registertcpserverport`: Parameter, der die Registrierung des Absenderports des IP-Pakets bei Verbindungen über das TCP-Protokoll aktiviert oder deaktiviert. Dieser Parameter kann die folgenden Werte annehmen:
  - `on`: Absenderport nicht registrieren. In diesem Fall werden die Einträge der Logdatei nach dem Empfängerport gruppiert.
  - `off` (Standardwert): Absenderport registrieren.

4. Drücken Sie die Tastenkombination **Strg+O**, um die Konfigurationsdatei zu speichern, und drücken Sie anschließend die Taste **Eingabe**.
5. Drücken Sie die Tastenkombination **Strg+X**, um die Datei zu schließen.

Logdatei registrierter IP-Pakete anzeigen

Die Logdatei registrierter IP-Pakete enthält Daten über offene und verschlüsselte IP-Pakete, die vom ViPNet Coordinator HW/VA-Netzwerkschutztreiber auf allen Netzwerkadaptern des betroffenen Computers verarbeitet wurden. Diese Daten können nützlich sein, um den Traffic

bestimmter Knoten zu überwachen oder um Verbindungsstörungen zwischen den Knoten zu beseitigen.

Führen Sie die folgenden Schritte aus, um die Logdatei der registrierten IP-Pakete anzuzeigen:

1. Führen Sie im Kommandointerpreter den Befehl `iplir view` aus.
2. Geben Sie im Fenster **Set search parameters** die Suchparameter für die Einträge in der Logdatei der registrierten IP-Pakete an. Sie können die folgenden Parameter angeben:
   - Zeitintervall, innerhalb von dem IP-Pakete registriert wurden,
   - Netzwerkadapter, auf denen IP-Pakete registriert wurden,
   - Verbindungsparameter (Verbindungsrichtung, Quell- und Zieladressen und -ports),
   - Ereignis, das bei der Verarbeitung des IP-Pakets registriert wurde,
   - andere Parameter.

   Standardmäßig werden alle Einträge gesucht, die innerhalb der letzten drei Stunden registriert wurden.

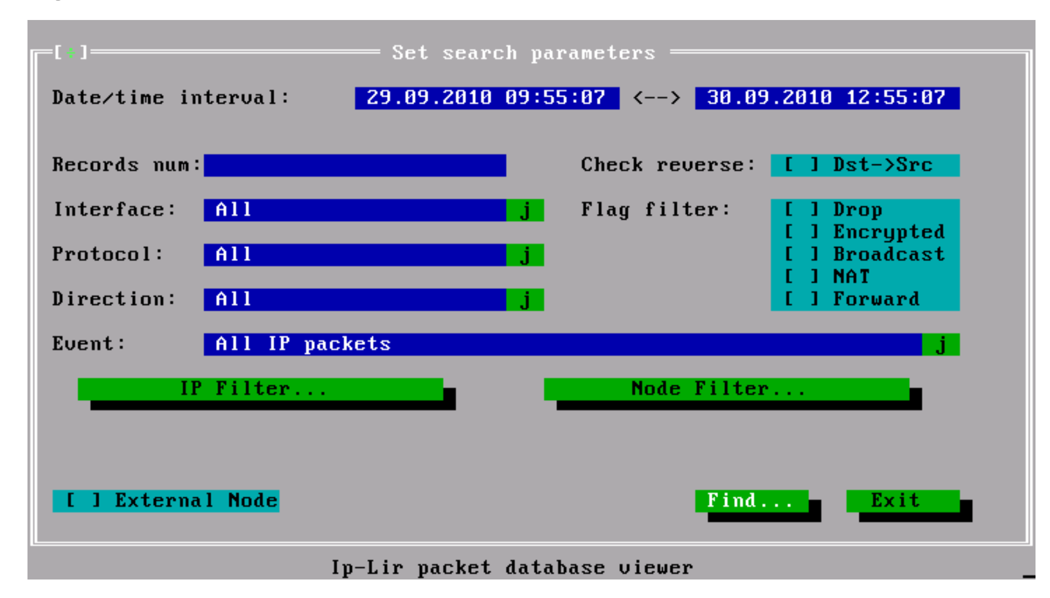
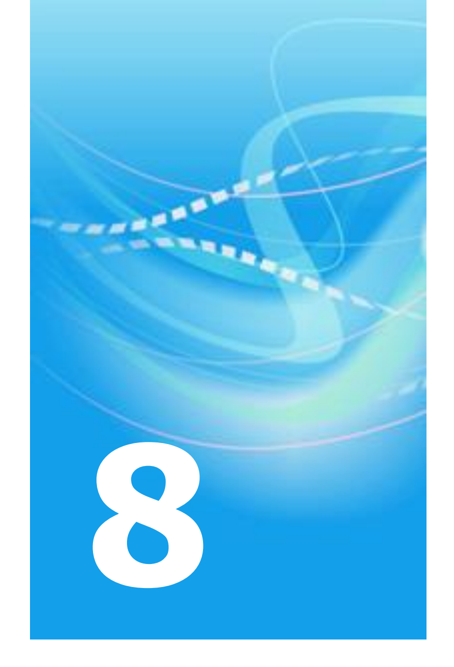


Abbildung 36: Einstellung der Suchparameter in der Logdatei der registrierten IP-Pakete

3. Klicken Sie auf die Schaltfläche **Find**. Die Suchergebnisse werden im Fenster **View results** eingeblendet.
4. Wenn Sie ausführliche Informationen über irgendein Ereignis anzeigen lassen wollen, wählen Sie den benötigten Eintrag in der Liste aus und drücken Sie die **Eingabe**-Taste.

Ausführliche Informationen zur Anzeige der Logdatei registrierter IP-Pakete sind im Dokument „ViPNet Coordinator HW/VA. Referenzhandbuch“ enthalten.



Zuverlässiger Zugang zu Netzwerkressourcen durch Verwendung alternativer Traffic-Kanäle

Über Verwendung alternativer Datenübertragungskanäle

Wenn Sie den Zugang zu einem Netzwerk oder zu einer Webressource verbessern möchten, können Sie zwei unabhängige Kanäle einrichten, die sich im Fall von Störungen gegenseitig dublieren oder einen Lastenausgleich des Traffics durchführen können. Sie können z. B. zwei Anbieter für den Internetzugang verwenden, um mögliche Verbindungsstaus und Ausfälle zu reduzieren. Dieser Ansatz ermöglicht es, eine gleichmäßige Verteilung des Traffics durchzuführen und einen zusätzlichen Reservekanal für Internetverbindungen zu verwenden. Die Verwendung alternativer Kanäle wird vom *loadbalancer* gesteuert.

Hinweis. Alternative Kanäle können ausschließlich für nicht verschlüsselte (nicht-VPN) Verbindungen verwendet werden. Gegenwärtig unterstützt der Dienst zwei alternative Kanäle vom Typ Ethernet.

Die Verwendung alternativer Kanäle kann in den folgenden Modi aktiviert werden:

- Redundanzmodus: in diesem Fall wird einer der zwei Kanäle als Primärkanal festgelegt. Wenn dieser Kanal ausfällt, dann wird der Traffic über den alternativen Kanal weitergeleitet. In diesem Fall wird die Verbindung über den Primärkanal regelmäßig überprüft. Sobald der Primärkanal betriebsbereit ist, wird der Traffic wieder über den Primärkanal geleitet.
- Traffic-Lastenausgleichsmodus. In diesem Fall wird der Traffic gemäß den von Ihnen festgelegten Prioritäten auf die zwei Kanäle aufgeteilt. Sie können z. B. für einen der Kanäle eine Traffic-Rate von 80 % definieren. Der Rest des Traffics wird über den anderen Kanal weitergeleitet. Wenn einer der Kanäle ausfällt, wird der Traffic zu 100 % über den störungsfreien Kanal solange weitergeleitet, bis der gestörte Kanal wieder betriebsbereit ist.

Wenn die Verwendung alternativer Kanäle aktiviert ist, überprüft der Dienst *loadbalancer* regelmäßig die Verfügbarkeit der beiden Kanäle, indem er versucht, auf die Test-IP-Adresse zuzugreifen. Der Dienst versucht dabei, mit Hilfe einer ICMP-Anfrage auf die Testadresse eines der beiden Kanäle abwechselnd zuzugreifen. Wenn der Zugriff auf die Testadresse über einen bestimmten Kanal erfolgreich verläuft, dann bedeutet das, dass der entsprechende Kanal aktiv ist. Wenn der Zugriff fehlschlägt, dann wird der entsprechende Kanal als fehlerhaft eingestuft. Wenn beide Kanäle ausfallen, dann setzt der Dienst seine regelmäßigen Überprüfungen

trotzdem fort. Sobald einer der Kanäle wieder betriebsbereit ist, wird der Traffic automatisch über diesen Kanal weitergeleitet.

Beim Konfigurieren des Dienstes *loadbalancer* müssen Sie eine Test-IP-Adresse festlegen, die über beide Kanäle erreichbar sein sollte, sobald diese Kanäle verfügbar sind.

Konfiguration des Dienstes loadbalancer im Redundanzmodus

Gehen Sie wie folgt vor, um den Redundanzmodus auf dem ViPNet Coordinator HW/VA-Knoten zu konfigurieren:

1. Wechseln Sie in der Befehlszeilenschnittstelle in den Administratormodus mit Hilfe des Befehls `enable`.
2. Stoppen Sie den Dienst *loadbalancer* durch Ausführen des Befehls `service loadbalancer stop`.
3. Aktivieren Sie den Redundanzmodus durch Ausführen des Befehls `service loadbalancer set mode failover`.
4. Fügen Sie die zwei Kanäle hinzu und konfigurieren Sie diese:
   - **4.1** Legen Sie den Namen des ersten Kanals mit Hilfe des Befehls `service loadbalancer add provider <Name>` fest.
   - **4.2** Legen Sie das Standardgateway des ersten Kanals durch Ausführen des Befehls `service loadbalancer set provider <Name> gateway <IP-Adresse>` fest.
   - **4.3** Legen Sie den Netzwerkadapter des Knotens, der mit dem ersten Kanal verbunden werden soll, mit Hilfe des Befehls `service loadbalancer set provider <Name> interface <Netzwerkadapter>` fest.
   - **4.4** Wiederholen Sie die aufgeführten Schritte für die Konfiguration des zweiten Kanals.
5. Legen Sie den Standardkanal durch Ausführen des Befehls `service loadbalancer set provider <Name> default` fest. Wenn dieser Kanal verfügbar ist, wird der gesamte Traffic über diesen Kanal geleitet.
6. Geben Sie die Test-IP-Adresse (s. Über Verwendung alternativer Datenübertragungskanäle auf S. 120) (die für die Verfügbarkeitsüberprüfung des Kanals verwendet wird) mit Hilfe des Befehls `service loadbalancer set testip <IP-Adresse>` an.
7. Definieren Sie das Abrufintervall für die Testadresse (zwischen 10 und 600 Sekunden) durch Ausführen des Befehls `service loadbalancer set polltime <time>`. Das Standardintervall beträgt 10 Sekunden.
8. Wenn das ViPNet Coordinator HW/VA Quellübersetzung (NAT) für interne Netzwerke durchführen soll, dann aktivieren Sie das mit Hilfe des Befehls `service loadbalancer`

`nat add localnet <Netzwerk>`, wobei `<Netzwerk>` ist Netzwerk-IP-Adresse im CIDR-Format an, z. B. `192.168.0.0/24`.

Achtung! Damit NAT ordnungsgemäß funktioniert, sollten entsprechende Firewall-Einstellungen vorgenommen werden. Sie können dies nach dem Abschluss der Konfiguration des Dienstes *loadbalancer* tun.

9. Aktivieren Sie den automatischen Start des Dienstes *loadbalancer* beim Starten des Knotens durch Ausführen des Befehls `service loadbalancer mode on`.
10. Wenn Sie den Dienst *loadbalancer* sofort (ohne Neustart des Appliance) starten möchten, führen Sie den Befehl `service loadbalancer start` aus.

Weitere Informationen über den Dienst *loadbalancer* und über das Erstellen, Bearbeiten und Löschen der Kanäle finden Sie im Dokument „ViPNet Coordinator HW/VA. Referenzhandbuch“.

Konfiguration des Dienstes loadbalancer im Traffic-Lastenausgleichsmodus

Gehen Sie wie folgt vor, um den Traffic-Lastenausgleichsmodus auf dem ViPNet Coordinator HW/VA-Knoten zu konfigurieren:

1 Wechseln Sie in der Befehlszeilenschnittstelle in den Administratormodus mit Hilfe des Befehls `enable`.

2 Stoppen Sie den Dienst *loadbalancer* durch Ausführen des Befehls `service loadbalancer stop`.

3 Aktivieren Sie den Dienst *loadbalancer* durch Ausführen des Befehls `service loadbalancer set mode balancing`.

4 Fügen Sie die zwei Kanäle hinzu und konfigurieren Sie diese:

4.1 Legen Sie den Namen des ersten Kanals mit Hilfe des Befehls `service loadbalancer add provider <Name>` fest.

4.2 Legen Sie das Standardgateway des ersten Kanals durch Ausführen des Befehls `service loadbalancer set provider <Name> gateway <IP-Adresse>` fest.

4.3 Legen Sie den Netzwerkadapter des Knotens, der mit dem ersten Kanal verbunden werden soll, mit Hilfe des Befehls `service loadbalancer set provider <Name> interface <Netzwerkadapter>` fest.

4.4 Legen Sie das Lastgewicht des ersten Kanals mit Hilfe des Befehls `service loadbalancer set provider <Name> weight <Gewicht>` fest. Das Lastgewicht bestimmt den Anteil des Traffics, der über den gegebenen Kanal geleitet wird. Benutzen Sie einen ganzzahligen Wert zwischen 1 und 10.

Das Verhältnis der Lastgewichte der beiden Kanäle bestimmt ihren jeweiligen Anteil des übermittelten Traffics. Wenn Sie den zwei Kanälen z. B. die Gewichte 2 und 4 zuweisen, dann wird ein Drittel des Traffics über den ersten Kanal und der Rest über den zweiten Kanal geleitet. Wenn Sie die Gewichte 3 und 6 zuweisen, bleibt das Verhältnis der Lastenverteilung gleich, d. h. ein Drittel zu zwei Drittel.

4.5 Führen Sie die gleichen Schritte zum Hinzufügen und Konfigurieren des zweiten Kanals aus.

5 Geben Sie die Test-IP-Adresse (s. Über Verwendung alternativer Datenübertragungskanäle auf S. 120) (die für die Verfügbarkeitsüberprüfung des Kanals

verwendet wird) mit Hilfe des Befehls `service loadbalancer set testip <IP-Adresse>` an.

6 Definieren Sie das Abrufintervall für die Testadresse (zwischen 10 und 600 Sekunden) durch Ausführen des Befehls `service loadbalancer set polltime <time>`. Das Standardintervall beträgt 10 Sekunden.

7 Wenn das ViPNet Coordinator HW/VA Quellübersetzung (NAT) für interne Netzwerke durchführen soll, dann aktivieren Sie das mit Hilfe des Befehls `service loadbalancer nat add localnet <Netzwerk>`, wobei `<Netzwerk>` ist Netzwerk-IP-Adresse im CIDR-Format an, z. B. `192.168.0.0/24`.

Achtung! Damit NAT ordnungsgemäß funktioniert, sollten entsprechende Firewall-Einstellungen vorgenommen werden. Sie können dies nach dem Abschluss der Konfiguration des Dienstes *loadbalancer* tun.

8 Aktivieren Sie den automatischen Start des Dienstes *loadbalancer* beim Starten des Knotens durch Ausführen des Befehls `service loadbalancer mode on`.

9 Wenn Sie den Dienst *loadbalancer* sofort (ohne Neustart des Appliance) starten möchten, führen Sie den Befehl `service loadbalancer start` aus.

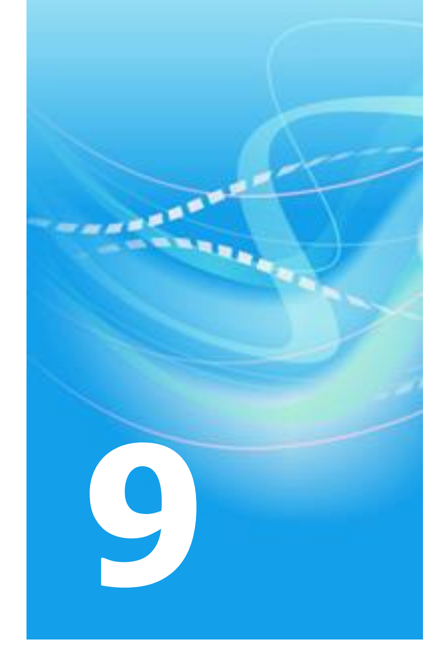
Weitere Informationen über den Dienst *loadbalancer* und über das Erstellen, Bearbeiten und Löschen der Kanäle finden Sie im Dokument „ViPNet Coordinator HW/VA. Referenzhandbuch“.

Logdatei der alternativen Kanäle

Alle Ereignisse, die mit der Verwendung alternativer Datenübertragungskanäle in Zusammenhang stehen, werden in der System-Logdatei `everything.log` protokolliert. Folgende Ereignisse werden erfasst:

- Ausfall eines Kanals;
- Wiederherstellung eines Kanals;
- Umschalten zwischen den Kanälen.

Die Logdatei kann durch Ausführen des Befehls `machine show logs` angezeigt werden.



Failover-System

Zweckbestimmung des Failover-Systems

Ein Failover-System ist für den Aufbau einer fehlertoleranten Softwarelösung auf Basis der Software ViPNet Coordinator HW/VA vorgesehen. Dieses System kann in zwei Modi agieren:

1. Single-Modus (das System ist auf einem separaten Server implementiert).

   Bei der Arbeit im Single-Modus führt das Failover-System Funktionen aus, die die dauernde Funktionsfähigkeit von im Softwarepaket beinhalteten grundliegenden ViPNet Diensten gewährleisten:

   - Ständige Überprüfung des Dienstzustandes und Führung der Statistik über Systemressourcennutzung;
   - Erkennung der Dienststörungen und die Durchführung der nachhaltigen Versuche, die Funktion der abgestützten Anwendung wiederherzustellen;
   - Vorbeugung von internen Störungen im Failover-System;
   - Neustart des Systems beim Ausfall des VPN-Netzwerkschutztreibers.

2. Cluster-Modus (das System ist auf einem Hochverfügbarkeitscluster eingerichtet).

   Ein Failover-Cluster besteht aus zwei Knoten (Clusterknoten), die miteinander verbunden sind und die Funktionalität des jeweils anderen Knotens gegenseitig duplizieren. Bei einem der Clusterknoten handelt es sich um einen aktiven Knoten. Dieser Knoten tritt als Coordinator (ViPNet Coordinator) (auf S. 242) auf. Der andere Knoten ist passiv und befindet sich im Standby-Modus. Wenn es zu einem Ausfall des aktiven Knotens kommt, dann wird der betroffene Knoten in den passiven Modus gesetzt. Der andere Knoten wird aktiv und übernimmt die Funktionen des ausgefallenen Knotens.

   Wenn das Failover-System im Cluster-Modus arbeitet, gewährleistet es die Verfügbarkeit der grundlegenden ViPNet Dienste auf die gleiche Art und Weise wie im Single-Modus.

Hinweis. Das Failover-System im Cluster-Modus (s. Failover-System auf S. 127) ist nur für Coordinator VA-Modifikationen verfügbar (s. Unterstützte ViPNet Coordinator HW/VA-Plattformen auf S. 12).

Nachfolgend finden Sie die Richtlinien für die Konfiguration des Servers im Single-Modus. Informationen zur Arbeit im Cluster-Modus finden Sie im Dokument „ViPNet Coordinator HW/VA. Failover-System. Administratorhandbuch“.

Hinweis. Im Cluster-Modus sind einige Dienste von ViPNet Coordinator HW/VA nicht verfügbar (s. Nicht verfügbare Dienste im Cluster-Modus auf S. 130).

Nicht verfügbare Dienste im Cluster-Modus

Im Cluster-Modus sind folgende Funktionen von ViPNet Coordinator HW/VA (s. Hauptfeatures auf S. 15) nicht verfügbar:

- Netzwerkfunktionen:
  - Wi-Fi Access Point;
  - 3G/LTE-Modem;
- Dienste:
  - DHCP;
  - HTTP/FTP-Proxyserver inklusive Webinhaltsfilter und Antivirus-Dienste;
  - IPsec-Server;
  - VoIP-Server.
- Überwachung von ViPNet Coordinator HW/VA:
  - SNMP.

Wenn das Failover-System im Single-Modus arbeitet und dabei eine der aufgeführten Funktionen aktiviert wird, dann kann das System nicht in den Cluster-Modus gesetzt werden, bis diese Dienste oder Features wieder deaktiviert sind. Wenn Sie den Cluster-Modus aktivieren, werden Sie gefragt, ob das System diese Dienste und Features automatisch deaktivieren soll.

Funktionsprinzipien des Failover-Systems im Single-Modus

Im Single-Modus wird die Funktionsfähigkeit von ViPNet Coordinator HW/VA durch die Überwachung folgender Elemente sichergestellt:

- Systemintegrität: diese Überprüfung wird auf Kernel-Ebene durchgeführt, und zwar auch dann, wenn das System auf keine externen Ereignisse mehr reagiert. Die Überprüfung der Systemintegrität wird auch dann fortgesetzt, wenn Sie das Failover-System deaktivieren.

- Funktionsfähigkeit des ViPNet Steuerungsdaemons (*iplircfg*) und des MFTP-Moduls (*mftpd*). Wenn diese Dienste ausfallen, dann initiiert das Failover-System einen Wiederherstellungsvorgang für die betroffenen Anwendungen. Das Failover-System kann so konfiguriert werden, dass bei wiederholten Fehlern im System selbst oder in den überwachten Anwendungen ein automatischer Neustart des Appliance durchgeführt wird (s. Verwaltung des Failover-Systems auf S. 132).

Weitere Informationen zur Vorgehensweise des Failover-Systems im Fall von Ausfällen s. Dokument „ViPNet Coordinator HW/VA. Failover-System“.

Verwaltung des Failover-Systems

Im Single-Modus können Sie das Failover-System mit Hilfe folgender Befehle steuern:

- Führen Sie zum Starten des Failover-Systems den Befehl `failover start` aus.
- Führen Sie zum Anhalten des Failover-Systems den Befehl `failover stop` aus.
- Bearbeiten Sie zum Konfigurieren des Failover-Systems die Konfigurationsdatei des Systems. Führen Sie den Befehl `failover config edit` aus, um die Datei zum Bearbeiten zu öffnen.

  Im Bereich `[misc]` können Sie den Parameter `reboot` einstellen, der den automatischen Neustart des Systems im Fall von Störungen aktiviert (`yes`) oder deaktiviert (`no`).

  Im Bereich `[debug]` können Sie die folgenden Parameter konfigurieren:

  - `debuglevel` legt die Protokollierungsstufe der Logdatei fest. Der Parameter kann den Wert -1 oder eine Ganzzahl von 1 bis 5 aufweisen. Wenn der Parameterwert -1 beträgt, dann ist die Protokollierung deaktiviert.
  - `debuglogfile` legt den Speicherort der Logdatei im Format `syslog:<facility.level>` fest. Der Standardwert dieses Parameters ist `syslog:daemon.debug`.

Achtung! Wenn das Failover-System angehalten wurde und Sie versuchen, es durch die manuelle Ausführung des Befehls `failover start` auf einem ViPNet Coordinator HW/VA wieder zu starten, dann werden die überwachten Anwendungen (ViPNet Steuerungsdaemon und MFTP-Modul) nicht automatisch neu gestartet. Diese Anwendungen müssen mit Hilfe der Befehle `iplir start` und `mftp start` manuell neu gestartet werden.

Führen Sie einen der folgenden Schritte aus, um den Status des Failover-Systems anzuzeigen:

- Greifen Sie über die Webschnittstelle (s. Anmeldung an der Webschnittstelle auf S. 48) auf den Knoten zu und öffnen Sie dort die **Einstellungen des Systems**.
- Greifen Sie über die Befehlszeilenschnittstelle auf den Knoten zu und führen Sie dort den Befehl `failover show info` aus.

Weitere Informationen zur Arbeit mit dem Failover-System und zur Konfiguration eines Failover-Clusters (s. Zweckbestimmung des Failover-Systems auf S. 128) s. Dokument „ViPNet Coordinator HW/VA. Failover-System."

Verwendungsszenarien für ViPNet Coordinator HW/VA

ViPNet Coordinator HW/VA für Einrichtung des lokalen Netzwerks verwenden

ViPNet Coordinator HW/VA ermöglicht die schnelle und einfache Einrichtung eines lokalen Netzwerks für ein kleines Büro.

Beispiel: die Firma besitzt eine Filiale, in welcher ein Netzwerk aus mehreren Computern eingerichtet werden soll. Einige dieser Computer sollen über einen abgesicherten Verbindungskanal zur Zentrale verfügen, wo ein ViPNet Netzwerk installiert ist. Für die restlichen Computer wird lediglich der Zugang zum Internet benötigt.

Zum Lösen dieser Aufgabe sollte an der Grenze des lokalen Netzwerks ein Computer mit ViPNet Coordinator HW/VA-Software installiert werden. Dieser Computer sollte über mehrere Netzwerkadapter verfügen, von denen einer an das Internet und ein weiterer an das lokale Netzwerk angeschlossen wird.

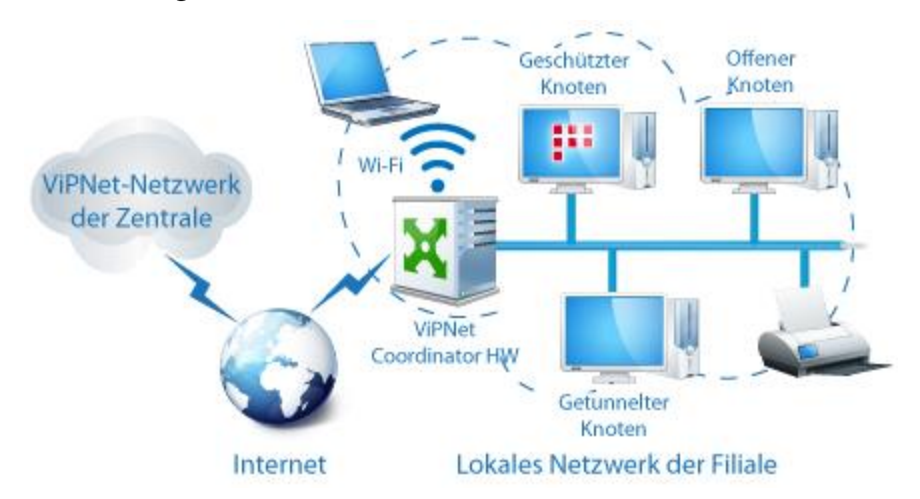


Abbildung 37: ViPNet Coordinator HW/VA für den Aufbau eines lokalen Netzwerks verwenden

Der als Coordinator (VPN-Server und Gateway) eingesetzte Knoten gewährleistet die Tunnelung bestimmter Knoten im LAN (getunnelte Knoten), wodurch diese Knoten auf Unternehmensressourcen im VPN der Hauptniederlassung zugreifen können (s. Bereitstellung eines sicheren Zugangs zu Ressourcen im Firmen-LAN aus anderen LANs (Site-to-Site Verbindung) auf S. 159). Wenn weitere ViPNet Knoten im LAN untergebracht sind (z. B.

ViPNet Clientknoten), dann können diese Knoten ebenfalls auf das VPN des Hauptsitzes zugreifen.

ViPNet Coordinator HW/VA kann im Netzwerk der Filiale folgende Funktionen erfüllen:

- Router, der die Übertragung von Daten zwischen dem lokalen Netzwerk und dem Internet sicherstellt;
- Wi-Fi-Access Point.
- Firewall, die Adressenübersetzung durchgeführt.

  Sie können Firewall zum blockeieren des Zugangs lokaler Netzwerkknoten ins Internet konfigurieren.

Hinweis. Die Knoten im LAN können nur dann auf das Internet zugreifen, wenn Sie zusätzlich den Netzwerkadapter des Coordinators auf der Seite des öffentlichen Netzwerks konfigurieren. Führen Sie dazu eine der folgenden Aktionen aus:

- ändern Sie die Sicherheitsstufe des Adapters von 2 (Standardstufe) auf 3 (s. Änderung der Sicherheitsstufe auf einem Netzwerkadaper auf S. 108);
- konfigurieren Sie Firewallregeln, die den Traffic der Knoten im LAN in Richtung Internet erlauben (s. Manuelle Konfiguration der integrierten Firewall für den Zugruiff des Netzwerkknoten ins Internet aus lokalem Netzwerk auf S. 167).

- DHCP-, NS- und NTP-Server für Computer des lokalen Netzwerks.
- Caching-Proxyserver mit Antivirus- und Inhaltskontrollfunktionen, der eine sichere Arbeit der Benutzer des lokalen Netzwerks im Internet sicherstellt und den Zugang zu unerwünschten Objekten einschränkt.
- VoIP-Server, der das SIP-Protokoll unterstützt. Mit Hilfe des VoIP-Servers können Sie ein firmeninternes IP-Telefoniesystem aufbauen und verschlüsselte Sprachkommunikation zwischen unterschiedlichen Niederlassungen Ihrer Firma ermöglichen.

Ein Beispiel für die Verwendung von ViPNet Coordinator HW/VA zum Installieren eines lokalen Netzwerks mit mehreren Segmenten ist im Abschnitt DMZ-Segment einrichten (auf S. 138) aufgeführt.

Vorgehensweise bei der Einrichtung des lokalen Netzwerks

Zum Einrichten eines lokalen Netzwerks mit Hilfe von ViPNet Coordinator HW/VA wird es empfohlen, alle Schritte aus der nachfolgenden Liste durchzuführen.

Tabelle 10. Lokales Netzwerk einrichten

	Aktion	Verweis
☐	Installieren Sie ViPNet Coordinator HW/VA. Führen Sie davor im Programm ViPNet Network Manager alle erforderlichen Netzwerkknoten-Einstellungen durch.	Installation von ViPNet Coordinator HW/VA (auf S. 28)
☐	Konfigurieren Sie die Verbindung des ViPNet Coordinator HW/VA-Netzwerkknotens zum Internet.	ViPNet Coordinator HW/VA zum Netzwerk verbinden (auf S. 60)
☐	Wenn erforderlich, konfigurieren Sie ViPNet Coordinator HW/VA für den Einsatz als Wi-Fi-Zugriffspunkt.	Parameter des Wi-Fi-Access Points einstellen (auf S. 82)
☐	Konfigurieren Sie die integrierten DHCP-, DNS-, NTP-Server für das Ethernet-Netzwerk.	Parameter des DHCP-Servers einstellen (auf S. 84) Parameter des DNS-Servers einstellen (auf S. 85) Parameter des NTP-Servers einstellen (auf S. 86)
☐	Konfigurieren Sie den integrierten Proxyserver, um den abgesicherten Zugang der Benutzer zum Internet sicherzustellen.	Konfiguration des Proxy-Servers (auf S. 89)
☐	Konfigurieren Sie die Regeln der Adressenübersetzung und die Transitregeln, um den Zugang lokaler Computer zum Internet zu gewährleisten.	Bearbeitungsregeln für offenen Traffic einstellen (auf S. 110)
☐	Wenn ein firmeninternes IP-Telefoniesystem installiert werden soll, konfigurieren Sie den eingebauten VoIP-Server.	Konfiguration des VoIP-Servers (auf S. 98)
☐	Wenn erforderlich, konfigurieren Sie zusätzliche Filterregeln für den offenen Traffic.	Bearbeitungsregeln für offenen Traffic einstellen (auf S. 110)

Tipp. Wir empfehlen, die Liste auszudrucken, und die einzelnen Schritte nach ihrer Durchführung zu markieren.

DMZ-Segment einrichten

Mit Hilfe von ViPNet Coordinator HW/VA kann ein höheres Maß an Schutz für das lokale Netzwerk erzielt werden, indem öffentliche Server, die unterschiedliche Dienste für externe Benutzer anbieten (E-Mail, Webserver, usw.), in ein eigenes Segment verschoben werden. Diese Maßnahme ermöglicht es, die Computer des lokalen Netzwerks im Fall von Attacken auf öffentliche Server zu schützen und einen störungsfreien Zugang zum Internet für alle Netzwerkbenutzer bereitzustellen.

Durch die Konfiguration einer Firewall (auf S. 243) auf einem ViPNet Coordinator HW/VA-Knoten kann das unternehmensinterne LAN in logische Segmente mit separat eingestellten Zugriffsrichtlinien unterteilt werden, ohne dass irgendwelche ViPNet Software auf den entsprechenden LAN-Knoten installiert werden muss. Beispielsweise kann das LAN in folgende zwei Segmente geteilt werden:

- Geschütztes Segment, in welchem sich Knoten befinden, für welche ausgehende Verbindungen zu externen Knoten im Internet erlaubt, eingehende Verbindungen von externen Knoten jedoch verboten sind. Die Knoten dieses Segments sind vor unerlaubten Zugriffen aus dem Internet geschützt.
- DMZ-Segment (s. DMZ (entmilitarisierte Zone) auf S. 243), in welchem sich Knoten befinden, für welche eingehende Verbindungen von externen Knoten im Internet über bestimmte Protokolle und Ports erlaubt sind. In diesem Segment können zum Beispiel Server untergebracht werden, auf die externe Benutzer zugreifen können.

Betrachten wir das folgende Beispiel:

- Das LAN soll in zwei Segmente geteilt werden: ein geschütztes Segment und eine DMZ (demilitarized zone).
- Ein Server innerhalb der DMZ soll vom Internet erreichbar sein (IP-Adresse 192.168.2.10, Port 80).
- Die IP-Adressen der Knoten im geschützten Segment stammen aus dem IP-Adressenpool 192.168.1.0/24.
- Der externe Netzwerkadapter des Coordinators besitzt die IP-Adresse 93.151.13.203.

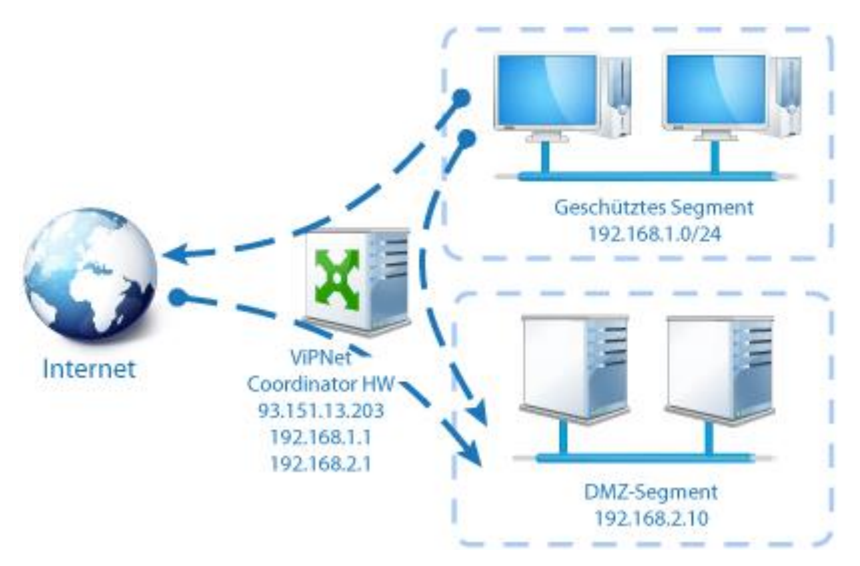


Abbildung 38: ViPNet Coordinator HW/VA für den Aufbau eines DMZ-Segments verwenden

Die beschriebene LAN-Segmentierung und Konnektivität können eingerichtet werden, indem Sie entsprechende Transitfilter und NAT-Regeln für den Traffic auf dem Coordinator konfigurieren:

1. Richten Sie ViPNet Coordinator HW/VA (s. Vorgehensweise bei der Installation von ViPNet Coordinator HW/VA auf S. 29) an der Grenze des lokalen Netzwerks.

2. Melden Sie sich in der Befehlszeilenschnittstelle (s. Verwalten von ViPNet Coordinator HW/VA-Knoten auf S. 46) von ViPNet Coordinator HW/VA.

3. Stoppen Sie den Steuerungsprogramm mit Hilfe des Befehls

   `iplir stop.`

4. Melden Sie such ins Administratormodus mit Hilfe des Befehls `enable`.

5. Führen Sie den folgenden Befehl aus, um die Konfigurationsdatei der Firewall zum Bearbeiten zu öffnen:

   ```
   iplir config firewall
   ```

6. Fügen Sie im Bereich `[forward]` die folgenden Regeln für Transit-IP-Pakete hinzu:

   - Regel, die ausgehende Verbindungen aus dem geschützten Segment zu beliebigen IP-Adressen über beliebige Protokolle erlaubt:

     ```
     rule= num 1 proto any from 192.168.1.0/24 to anyip pass
     ```

   - Regel, die Verbindungen in beiden Richtungen zwischen dem DMZ-Segment und beliebigen IP-Adressen über das HTTP-Protokoll erlaubt:

     ```
     rule= num 3 proto tcp from anyip to 192.168.2.10:80 pass
     ```

Der Parameter `num` legt die Priorität der Regel innerhalb des Bereichs fest.

Hinweis. Jeglicher Traffic, der nicht explizit erlaubt ist, wird blockiert. Es ist deshalb nicht nötig, eigene Regeln zu definieren, die den eingehenden Traffic an der Grenze des geschützten Segments blockieren.

---

7 Fügen Sie im Bereich `[nat]` folgende Regeln der Adressenübersetzung hinzu:

- Regel für die Einrichtung des Internet-Zugangs aus dem geschützten Segment:

```
rule= change src=93.151.13.203:dynamic proto any from 192.168.1.0/24 to
anyip
```

- Regel für die Einrichtung des Zugangs zum DMZ-Segment aus dem Internet:

```
rule= change dst=192.168.2.10:80 proto tcp from anyip to
93.151.13.203:80
```

8 Drücken Sie die Tastenkombination **Strg+O** und anschließend die **Eingabe**, um die Konfigurationsdatei zu speichern.

9 Drücken Sie die Tastenkombination **Strg+X**, um die Datei zu schließen.

10 Starten Sie den Daemon iplircfg mit Hilfe des Befehls `iplir start`.

11 Stellen Sie sicher, dass nach Durchführung dieser Einstellungen Verbindungen zwischen den Knoten in unterschiedlichen Segmenten des lokalen Netzwerks und des Internets in Übereinstimmung mit dem vorgegebenen Schema (s. Abbildung auf S. 139) hergestellt werden können.

Zugang zu einem ViPNet Coordinator HW/VA-Knoten durch Zuweisung der IP-Adressen-Aliase bereitstellen

Bei Bedarf können IP-Adressen-Aliase den Ethernet-Netzwerkadaptern eines ViPNet Coordinator HW/VA-Knotens zugewiesen werden.

Ein Ethernet-Adapter ist über seine IP-Adresse erreichbar (diese wird entweder vom DHCP-Server automatisch oder manuell zugewiesen). Wenn Sie IP-Aliase einem Adapter zuweisen, dann wird der Adapter auch über diese Aliase erreichbar sein.

Das Zuweisen der IP-Aliase ermöglicht die Konfiguration einer Vielzahl unterschiedlicher Zugriffsmethoden für den Zugang zum ViPNet Coordinator HW/VA-Knoten, z. B.:

- Damit ein ViPNet Coordinator HW/VA-Knoten über die Befehlszeilen- oder Webschnittstelle remote verwaltet werden kann (s. Verwalten von ViPNet Coordinator

HW/VA-Knoten auf S. 46), sollte dieser Knoten über seine IP-Adresse erreichbar sein. Da aber der Coordinator die IP-Adresse von einem DHCP-Server bezieht, ist diese IP-Adresse nicht konstant.

Durch die Zuweisung eines Alias an den Adapter, der seine IP-Adresse vom DHCP-Server bezieht, kann der Zugang zum Knoten über eine statische IP-Adresse sichergestellt werden.

- Beim Durchführen einer Segmentierung des LAN wird ein ViPNet Coordinator HW/VA-Knoten benötigt, der über Ethernet-Adapter auf der Seite des LAN-Segments und auf der Seite des Internet verfügt. Beispielsweise sollte der Knoten im DMZ-Schema über die Adressen 93.151.13.203, 192.168.1.1 und 192.168.2.1 verfügen, die seinen Adaptern zugewiesen sind.

  Dieses Schema kann allerdings auch dann implementiert werden, wenn der <Brand> -Knoten nur über einen Ethernet-Adapter verfügt. Es muss lediglich sichergestellt werden, dass jede der drei Adressen entweder die Haupt-IP-Adresse des Adapters oder einen seiner Aliase darstellt.

Betrachten wir das folgende Beispiel:

- Das LAN eines kleinen Büros enthält mehrere Computer, die über einen Router mit DHCP-Funktionalität auf das Internet zugreifen. Die Computer beziehen ihre IP-Adressen vom Router. Die zugewiesenen IP-Adressen stammen aus dem IP-Adressenpool 192.168.0.0/24.
- Mehrere Knoten und Geräte im LAN sollen auf geschützte Ressourcen in einem ViPNet VPN remote zugreifen. Im LAN befindet sich ein ViPNet Coordinator HW/VA-Knoten, der für die Tunnelung der Verbindungen dieser Knoten und Geräte beim Zugriff auf das Remote-VPN konfiguriert werden soll (s. Bereitstellung eines sicheren Zugangs zu Ressourcen im Firmen-LAN aus anderen LANs (Site-to-Site Verbindung) auf S. 159).
- Der ViPNet Coordinator HW/VA-Knoten verfügt über nur einen Ethernet-Adapter.
- Der ViPNet Coordinator HW/VA-Knoten soll remote über die Befehlszeilen- oder Webschnittstelle konfiguriert werden.

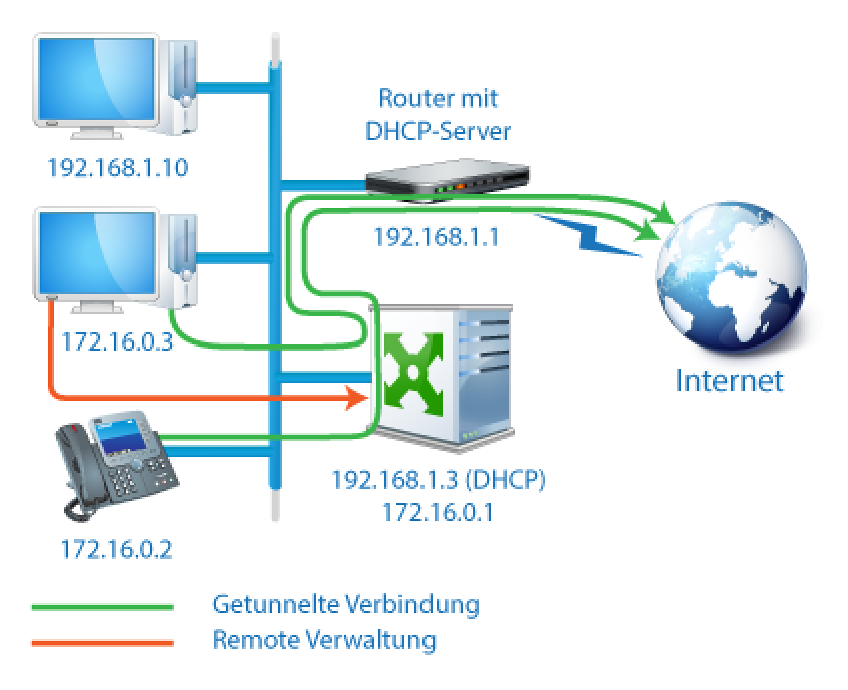


Abbildung 39: Verwendung zusätzlicher IP-Adressen

Gehen Sie wie folgt vor, um das beschriebene Schema zu implementieren:

1 Konfigurieren Sie den Bezug der IP-Adressen vom DHCP-Server auf dem Ethernet-Netzwerkadapter des ViPNet Coordinator HW/VA-Knotens (s. Verbindung zum Ethernet-Netzwerk herstellen auf S. 69). Auf dem Schema oben wurde dem Coordinator die Adresse 192.168.1.3 vom DHCP-Server zugewiesen.

2 Erstellen Sie ein separates Subnetz (172.16.0.0/24) für diejenigen LAN-Knoten, die mit dem VPN verbunden werden sollen:

2.1 Weisen Sie den getunnelten Knoten die IP-Adressen aus dem Subnetz 172.16.0.0/24 zu.

2.2 Legen Sie auf den getunnelten Knoten den Alias der IP-Adresse des Coordinators 172.16.0.1 als Standardgateway fest (dieser Alias wird dem Coordinator-Adapter zu einem späteren Zeitpunkt zugewiesen).

3 Konfigurieren Sie die Tunnelung im <Brand> Network Manager:

3.1 Fügen Sie den IP-Adressen-Alias 172.16.0.1 auf dem Netzwerkadapter des Coordinators hinzu (s. Verbinden zu einem Ethernet-Netzwerk mit Hilfe des ViPNet Network Manager auf S. 63).

3.2 Fügen Sie die IP-Adressen der vom Coordinator getunnelten Knoten zur Liste der getunnelten IP-Adressen hinzu (s. Konfiguration der Tunnelung auf einem ViPNet Coordinator HW/VA auf S. 67).

3.3 Senden Sie die Schlüssel an den Coordinator.

4 Aktivieren Sie die Remote-Konfiguration des ViPNet Coordinator HW/VA-Knotens von einem Knoten im LAN über die Web- oder Befehlszeilenschnittstelle.

- Weisen Sie dem Knoten, den Sie für die Remote-Konfiguration verwenden möchten, eine statische IP-Adresse zu.
- Konfigurieren Sie auf dem ViPNet Coordinator HW/VA-Knoten eine Filterregel für den offenen Traffic (s. Regeln zur Filterung des Traffics auf S. 112). Diese Regel soll alle eingehenden Verbindungen erlauben, die von dem Knoten stammen, der für die Remote-Konfiguration verwendet werden soll, und das HTTP-Protokoll (TCP-Port 80) oder das SSH-Protokoll (TCP-Port 22) verwenden. Beispiel:

```
rule= pass proto tcp from 172.16.0.3 to 172.06.0.1:22

rule= pass proto tcp from 172.16.0.3 to 172.06.0.1:80
```

Zentralisierten Proxyserver verwenden

Die Computer in einem LAN benötigen normalerweise den Schutz ihrer Verbindungen zum Internet durch einen Proxyserver.

Wenn mehrere LANs verwaltet werden, dann können diese jeweils durch eigene Proxyserver geschützt werden. Die Wartung dieser Proxyserver kann allerdings aufwändig sein. Um die Wartungskosten zu reduzieren, kann ein zentraler Proxyserver eingesetzt werden, der alle LANs zusammen schützt:

1. Installieren Sie in den jeweiligen LANs einen ViPNet Coordinator HW/VA-Knoten, der die Benutzeranforderungen an den zentralen Proxyserver über einen gesicherten ViPNet Tunnel weiterleiten soll (Durchführung der Tunnelung der Anforderungen).

2. Richten Sie einen ViPNet Coordinator HW/VA-Coordinator ein und verwenden dessen integrierten Proxyserverdienst dazu, die LANs zentralisiert zu schützen.

   Die gesamte Last der Verarbeitung von Benutzeranforderungen und Antivirus-Prüfungen wird vom zentralen Proxyserver übernommen. Dies erfordert einen beträchtlichen Umfang an Rechenleistung. Deswegen sollte ein Coordinator, der als zentraler Proxyserver eingesetzt werden soll, auf einem leistungsstarken High-End-Computer bereitgestellt werden.

Das vorgeschlagene Schema unterstützt den transparenten Proxyserver-Modus.

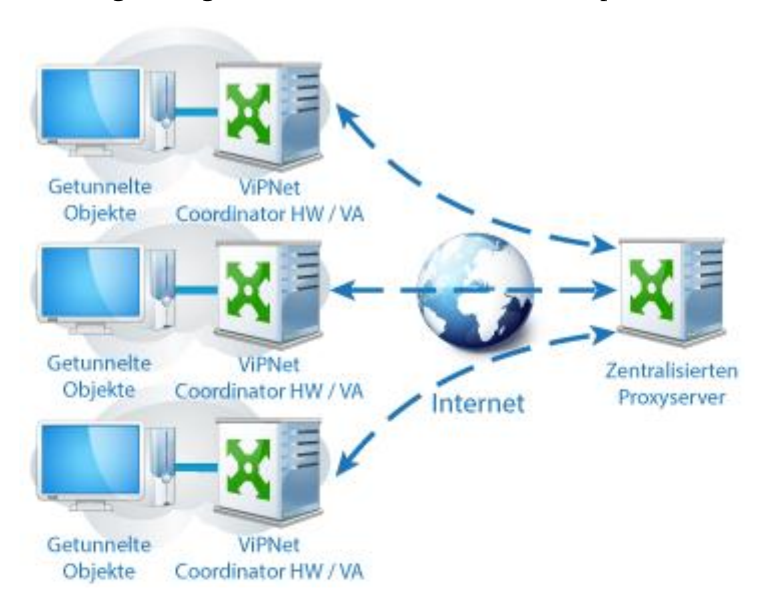


Abbildung 40: Schema mit dem zentralisierten Proxyserver

Zum Bereitstellen dieses Schemas:

1 Gehen Sie auf dem Knoten, der als zentraler Proxyserver eingesetzt werden soll, folgendermaßen vor:

   - Richten Sie das ViPNet Coordinator HW/VA-Appliance ein (s. Vorgehensweise bei der Installation von ViPNet Coordinator HW/VA auf S. 29);
   - Definieren Sie die Parameter des integrierten Proxyservers (s. Konfiguration der allgemeinen Proxyserver-Einstellungen auf S. 91);
   - Konfigurieren Sie bei Bedarf die Inhaltskontrolle (s. Inhaltskontrolle konfigurieren auf S. 94) und den Antivirus (s. Antivirus konfigurieren auf S. 97).

2 Konfigurieren Sie im ViPNet Network Manager die Tunnelung (s. Konfiguration der Tunnelung auf einem ViPNet Coordinator HW/VA auf S. 67) der Knoten im LAN durch ihre ViPNet Coordinator HW/VA-Knoten

3 Führen Sie auf den Knoten in den lokalen Netzwerken die erforderlichen Einstellungen durch:

   - Wenn der Proxyserver im normalen Modus verwendet werden soll, dann geben Sie in den Benutzeranwendungen (zum Beispiel im Webbrowser) der offenen und geschützten Knoten die IP-Adresse und den Port des zentralisierten Proxyservers an.
   - Wenn der Proxyserver im transparenten Modus verwendet werden soll, dann sollte auf jedem lokalen ViPNet Coordinator HW/VA-Server eine statische Regel der Adressenübersetzung (s. Regeln der Adressenübersetzung auf S. 114) im folgenden Format erstellt werden:

```
rule= proto tcp from <lokale IP> to any:<Internetobjekte-Ports> change
dst=<IP des zentralen Proxy-Servers>:<Proxy-Port>
```

     wo:

     - `lokale IP`: IP-Adressen lokaler Knoten, die den Proxyserver verwenden sollen,
     - `Internetobjekte-Ports`: Ports, die für den Zugang zu Internetobjekten verwendet werden,
     - `IP des zentralen Proxy-Servers`: sichtbare IP-Adresse des zentralen Proxyservers auf dem Coordinator des LAN,
     - `Port des zentralen Proxy-Servers`: Listening-Port des zentralen Proxyservers.

     Beispiel:

```
rule= proto tcp from 192.168.10.0/24 to any:(21,80, 443, 8080) change
dst=201.75.152.67:3128
```

Achtung! Auf geschützten ViPNet Knoten kann ein zentralisierter Proxyserver, der im transparenten Modus arbeitet, nicht verwendet werden.

Bereitstellung eines sicheren Zugangs zu Ressourcen im Firmen-LAN aus Remote-Netzwerkknoten (Client-to-Site Verbindung)

Im LAN Ihres Unternehmens können sich Knoten befinden, auf denen keine ViPNet Software installiert werden kann, wie z. B. Server, Netzwerkdrucker, mobile Geräte, POS-Terminals und andere (im Folgenden werden diese Knoten als „offene Knoten" bezeichnet). Nichtsdestotrotz können die Verbindungen mit diesen Knoten durch die Technologie der Tunneling (s. Tunnelung auf S. 247) abgesichert werden.

Die Tunnelung kann von einem ViPNet Coordinator HW/VA Knoten oder einem ViPNet Coordinator durchgeführt werden. Die Tunnelung ermöglicht das Herstellen verschlüsselter Verbindungen eines getunnelten Knotens im LAN des Unternehmens:

- mit <Brand> Knoten innerhalb und außerhalb des LAN;
- mit offenen Knoten in anderen LANs, die von anderen Coordinatoren getunnelt werden.

Der getunnelte Knoten sendet offen IP-Pakete an ViPNet Coordinator HW/VA. ViPNet Coordinator HW/VA verschlüsselt diese IP-Pakete und leitet sie an einen ViPNet Knoten oder einen Remote-ViPNet Coordinator weiter, der die Pakete dann entschlüsselt und an einen anderen getunnelten Knoten weiterleitet. ViPNet Coordinator HW/VA kann alle offenen Knoten tunneln, mit denen er über folgende Adapter verbunden ist:

- Ethernet;
- Wi-Fi, wenn der ViPNet Coordinator HW/VA-Knoten als ein Wi-Fi Access Point konfiguriert ist;

Tipp. Da die Traffic-Tunnelung einen Ver- und Entschlüsselungsprozess darstellt, benötigt sie eine beträchtliche Menge an Rechenkapazität. Wenn auf die getunnelten Knoten häufig zugegriffen werden soll, dann sollte eine entsprechend hohe Rechenkapazität zur Verfügung gestellt werden, indem Sie eine passende Ausführung der ViPNet Coordinator HW/VA Appliance auswählen (s. Unterstützte ViPNet Coordinator HW/VA-Plattformen auf S. 12).

Zugriff von einem Remote-ViPNet Knoten

Nehmen wir an, dass in einem korporativen LAN mehrere Server vorhanden sind, auf denen keine ViPNet Software installiert ist. So muss der Zugang zu diesen Servern allen Mitarbeiten gewährleistet werden, die sowohl im LAN als auch auswärts arbeiten.

Abbildung 41: Verwendung des ViPNet Coordinator HW/VA zur Tunnelung offener Netzwerkknoten

Um die Tunnelung von im Netz vorhandenen Servern mit dem ViPNet Coordinator HW/VA durchzuführen, gehen Sie wie folgt vor:

1. Richten Sie an der Grenze des Netzwerksegments (s. Grenze des lokalen Netzwerkes auf S. 244) ein ViPNet Coordinator HW/VA ein.

2. Stellen Sie im ViPNet Network Manager das ViPNet Coordinator HW/VA ein (s. Konfiguration der Netzwerkeinstellungen von ViPNet Coordinator HW/VA in ViPNet Network Manager auf S. 62). In der Registerkarte **Tunnelung** tragen Sie in **IP-Adressen von getunnelten Verbindungen** die Adresse der offenen Server ein, die getunnelt werden sollen.

3. Erzeugen Sie im ViPNet Network Manager die Knotenschlüssel und senden diese an die Netzwerknoten.

4. Machen Sie Folgendes auf den getunnelten Netzwerkknoten:

   - Als Standardgateway tragen Sie das ViPNet Coordinator HW/VA ein.
   - Geben Sie die statische Route an, damit der für den nicht geschützten Netzwerkknoten bestimmte Datenverkehr über den ViPNet Coordinator HW/VA geht.

     Führen Sie zum Beispiel auf einem getunnelten Knoten mit dem Betriebssystem Windows in der Kommandozeile den folgenden Befehl aus:

     ```
     route add <IP-Zieladresse> mask <Subnetzmaske> <Gateway-IP-Adresse
     (VSG)> -p
     ```

5 Prüfen Sie, dass Tunnelung korrekt funktioniert, indem Sie eine Verbindung zwischen einem beliebigen geschützten ViPNet Knoten und einem getunnelten Objekt herstellen.

Zugang von Remoteknoten ohne ViPNet Software, die über einen ViPNet Kanal installiert wurden

Nehmen wir an, im Firmennetzwerk existiert ein Anwendungsserver auf Cloud-Basis. Zu diesem Server sollten geschützte Verbindungen von Benutzern offener Knoten und verschiedener Geräte, die von einem Remote-Coordinator getunnelt werden, möglich werden.

Damit zwischen den offenen Knoten und dem Anwendungsserver geschützte Verbindungen eingerichtet werden können, sollte die Tunnelung dieser Knoten und des Servers mit Hilfe von ViPNet Coordinator HW/VA organisiert werden.

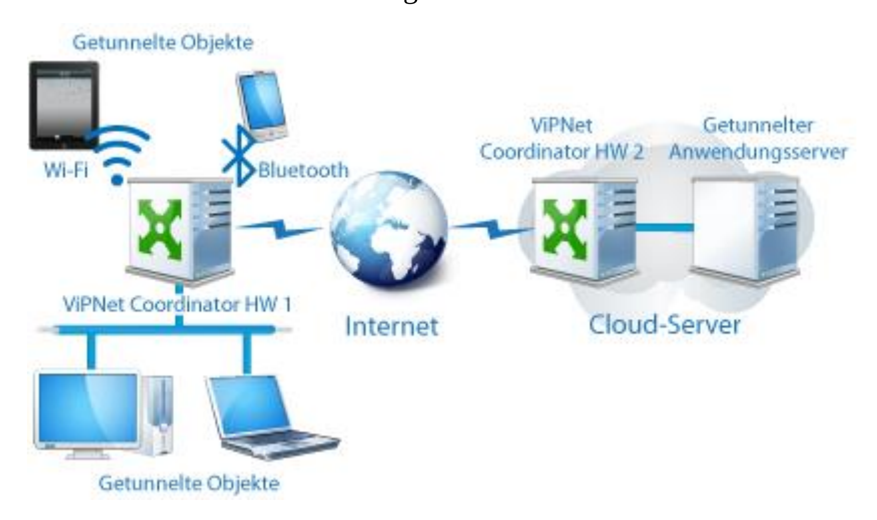


Abbildung 42: Geschützte Verbindungen zwischen offenen Knoten einrichten

Führen Sie die folgenden Schritte aus, um den ViPNet Coordinator HW/VA-Coordinator, der für die Tunnelung des Anwendungsservers („ViPNet Coordinator HW/VA 2“ in der Abbildung und im Folgenden) verwendet werden soll, zu konfigurieren:

1 Installieren Sie an der Grenze des Netzwerksegments (s. Grenze des lokalen Netzwerkes auf S. 244), in welchem sich der offene Anwendungsserver befindet, einen Coordinator ViPNet Coordinator HW/VA 2. Dieser Coordinator sollte über eine statische IP-Adresse oder DNS-Namen aus dem externen Netzwerk ansprechbar sein.

2 Führen Sie im Programm ViPNet Network Manager die Konfiguration des des ViPNet Coordinator HW/VA-Coordinators für die Tunnelung des Anwendungsservers durch (s. Konfiguration der Netzwerkeinstellungen von ViPNet Coordinator HW/VA in ViPNet Network Manager auf S. 62). Fügen Sie auf der Registerkarte **Tunnelung** in der

Liste **IP-Adressen der getunnelten Verbindungen** den Adressenbereich des offenen Anwendungsservers, der getunnelt werden soll, hinzu.

3 Führen Sie auf dem getunnelten Server eine der folgenden Aktionen aus:

  - Geben Sie als Standardgateway den Coordinator ViPNet Coordinator HW/VA 2 an.
  - Definieren Sie eine statische Route für den Traffic, der für offene Knoten bestimmt ist, indem Sie diesen über den Coordinator ViPNet Coordinator HW/VA 2 leiten.

    Führen Sie zum Beispiel auf dem getunnelten Server mit Betriebssystem Windows den folgenden Kommandozeilenbefehl aus:

    ```
    route add <IP-Zieladresse> mask <Subnetzmaske> <IP-Adresse von ViPNet
    Coordinator HW/VA 2> -p,
    ```

    wo `<IP-Zieladresse>` gleich dem Bereich virtueller IP-Adressen auf dem Coordinator ViPNet Coordinator HW/VA 2 ist.

Für die Tunnelung offener Knoten, die sich zum Anwendungsserver verbinden werden, führen Sie folgende Einstellungen des ViPNet Coordinator HW/VA:

1 Installieren Sie an der Grenze des Netzwerksegments (s. Grenze des lokalen Netzwerkes auf S. 244), in welchem sich die offenen Knoten befinden, einen ViPNet Coordinator HW/VA 1.

2 Führen Sie im Programm ViPNet Network Manager die Konfiguration des ViPNet Coordinator HW/VA 1 durch (s. Konfiguration der Netzwerkeinstellungen von ViPNet Coordinator HW/VA in ViPNet Network Manager auf S. 62). Geben Sie beim Einstellen die folgenden Parameter an:

  - Konfigurieren Sie in der Registerkarte **Firewall** Verbindungen über die Firewall mit dynamischem NAT; geben Sie als Coordinator für eingehende Verbindungen den Coordinator ViPNet Coordinator HW/VA 2 an.
  - Fügen Sie in der Registerkarte **Tunnelung** in der Liste **IP-Adressen der getunnelten Verbindungen** die Adressen offener Knoten, die getunnelt werden sollen, hinzu:
    - Für Geräte, die sich über das Wi-Fi-Protokoll verbinden (s. Parameter des Wi-Fi-Access Points einstellen auf S. 82), fügen Sie die einzelne Adresse aus dem Adressbereich 192.168.20.2-192.168.20.20 hinzu.
    - Für Geräte, die über das Ethernet verbunden sind, können Sie weitere beliebige Adressen oder Adressbereiche hinzufügen.
  - Verbinden Sie ViPNet Coordinator HW/VA 1 mit <Crtf_Product_name> 2.

3 Führen Sie auf den getunnelten Knoten eine der folgenden Aktionen aus:

  - Geben Sie als Standardgateway den Coordinator ViPNet Coordinator HW/VA 1 an.

- Definieren Sie eine statische Route für den Traffic, der für den offenen Anwendungsserver bestimmt ist, indem Sie diesen über den Coordinator ViPNet Coordinator HW/VA 1 leiten.

  Führen Sie zum Beispiel auf dem getunnelten Server mit Betriebssystem Windows den folgenden Kommandozeilenbefehl aus:

  ```
  route add <IP-Zieladresse> mask <Subnetzmaske> <IP-Adresse von ViPNet
  Coordinator HW/VA 1> -p
  ```

Wenn alle Einstellungen korrekt vorgenommen wurden, dann werden nun mit Hilfe der Technologie der Tunnelung geschützte Verbindungen zwischen dem offenen Anwendungsserver und anderen Knoten eingerichtet.

Bereitstellung eines sicheren Zugangs zum Firmen-LAN von mobilen Geräten über IPsec-Kanäle

Moderne Geschäftsprozesse sehen einen aktiven Einsatz mobiler Endgeräte vor. Mit Hilfe von mobilen Geräten können Mitarbeiter, die sich nicht an ihren Arbeitsplätzen befinden, das betriebliche E-Mail-System, die Möglichkeiten der IP-Telefonie oder andere Ressourcen des Firmennetzwerks nutzen.

Die Benutzer können unterschiedliche Smartphones und Tablets verwenden, um den geschützten Zugriff auf Unternehmensressourcen, die sich in einem ViPNet Netzwerk befinden, sicherzustellen. Der Schutz des Traffics wird dabei mit Hilfe einer Kombination der IPSec- und der ViPNet Technologie sichergestellt.

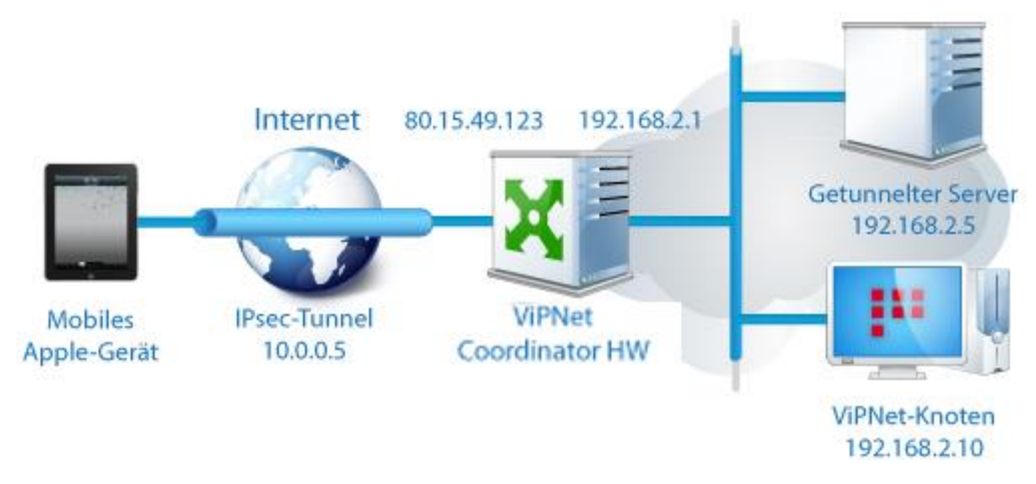


Abbildung 43: Mobiles Apple-Gerät beim Aufbau der Verbindung zum ViPNet Security Gateway

Ein ViPNet Coordinator HW/VA-Knoten wird als Gateway zwischen IPsec und ViPNet eingesetzt und ermöglicht den Zugang mobiler Geräte zu getunnelten und geschützten ViPNet Knoten. Das mobile Gerät baut dabei eine Verbindung zum ViPNet Coordinator HW/VA über das IPsec-Protokoll auf.Es wird ein gesicherter Client-to-Site IPsec-Kanal erstellt und dem mobilen Gerät automatisch eine IP-Adresse aus dem Netzwerkbereich 192.168.30.0/24 zugewiesen. Der Traffic des mobilen Geräts wird vom ViPNet Coordinator HW/VA-Knoten entschlüsselt. Dann wird der unverschlüsselte Traffic entweder zu einem offenen Knoten hinter dem ViPNet Coordinator HW/VA weitergeleitet oder mit ViPNet Schlüsseln verschlüsselt und an einen geschützten ViPNet Knoten übermittelt. Knoten, die sich im geschützten Netzwerk

hinter dem ViPNet Coordinator HW/VA befinden, können über ihre IP-Adressen von den mobilen Geräten angesprochen werden.

Die mobilen Geräte, die über das IPsec-Protokoll mit dem ViPNet Coordinator HW/VA verbunden sind, verwenden ViPNet Coordinator HW/VA als ihr Standardgateway. Wenn die Konfiguration nicht ordnungsgemäß durchgeführt wird, dann können diese Geräte auf die Ressourcen des Unternehmensnetzwerks, nicht jedoch auf das Internet zugreifen. Wenn zusätzlich der Zugang mobiler IPsec-Clients zum Internet eingerichtet werden soll, können Sie dazu den integrierten Proxyserver verwenden oder NAT-Regeln auf dem ViPNet Coordinator HW/VA-Knoten konfigurieren (s. Bereitstellung des Internetzugangs für mobile Geräte während der IPsec-Sitzungen auf S. 157).

ViPNet Coordinator HW/VA unterstützt bis zu 40 gleichzeitige Client-to-Site IPsec-Verbindungen. Darüber hinaus kann die Anzahl der mobilen Clients im ViPNet Netzwerk durch die ViPNet VPN-Lizenz begrenzt sein.

Die Basiseinstellungen, die Sie im Programm ViPNet Network Manager konfigurieren sollten, gelten sowohl für Apple- als auch für Android-Geräte (s. Anbindung mobiler Apple-Geräte auf S. 153). Der Unterschied besteht darin, dass IPsec-Einstellungen für iPad- und iPhone-Geräte mit Hilfe von ViPNet Network Manager bequem automatisch konfiguriert werden können, während Android-Geräte eine manuelle Konfiguration erfordern (s. Anbindung mobiler Android-Geräte auf S. 156).

Anbindung mobiler Apple-Geräte

Damit mobile Apple-Geräte auf geschützte Ressourcen im Unternehmensnetzwerk zugreifen können, sollten IPsec-Verbindungseigenschaften in ViPNet Network Manager konfiguriert werden. Dazu:

1 Wählen Sie im Programm ViPNet Network Manager in der Navigationsleiste den ViPNet Coordinator HW/VA-Knoten aus, der die Rolle des IPsec-Gateways übernehmen soll.

Achtung! Wenn Sie auf dem ViPNet Coordinator HW/VA-Knoten noch keine Schlüsseldistribution installiert haben und eine automatische Schlüsselinstallation durchführen möchten (s. Automatische Installation der Schlüsseldistribution auf S. 38), dann sollten Sie die IPsec-Verbindungseinstellungen erst nach der erfolgten Installation der Schlüssel konfigurieren.

---

2 Wenn Sie den gegebenen ViPNet Coordinator HW/VA-Knoten noch nie zuvor als IPsec-Gateway konfiguriert haben, dann führen Sie auf der Registerkarte **IPsec-Verbindung** die folgenden Schritte durch:

2.1 Wählen Sie in der Liste **Netzwerkadapter-Name** den Netzwerkadapter auf dem ViPNet Coordinator HW/VA-Knoten aus, der aus dem Internet angesprochen werden kann.

2.2 Aktivieren Sie das Kontrollkästchen **Coordinator als IPsec-Gateway für Anbindung von Smartphone-Clients verwenden**.

2.3 Geben Sie im Feld **IP-Adresse oder DNS-Name des Gateways** die öffentliche IP-Adresse oder den DNS-Namen ein, über welche eine Verbindung zum ViPNet Coordinator HW/VA aus dem Internet hergestellt werden kann.

2.4 Geben Sie im Feld **Pre-Shared Key** eine beliebige Reihenfolge an Zeichen ein (8 bis 63 Zeichen lang). Diese Zeichenfolge wird als Passwort für die Verbindungsauthentifizierung verwendet.

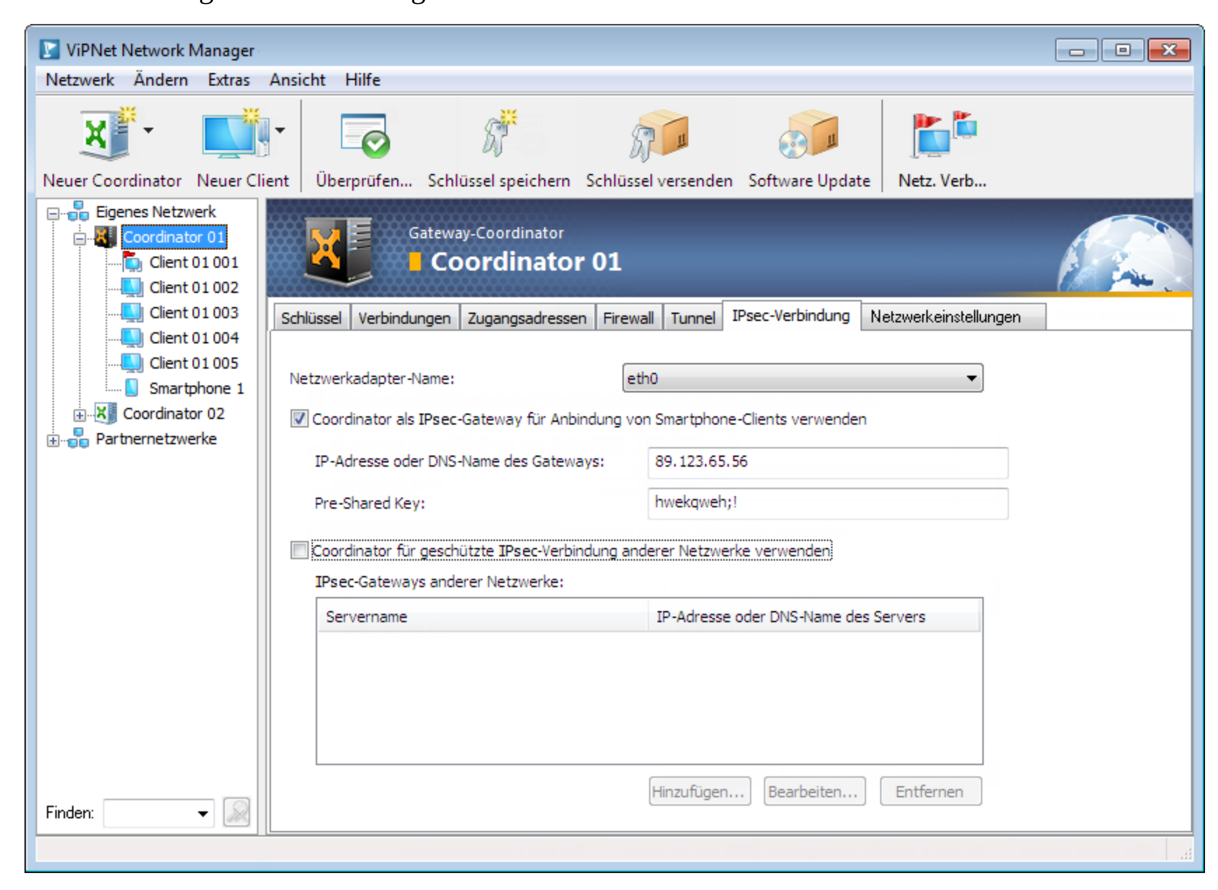


Abbildung 44: Konfiguration der IPsec-Verbindungsparameter für den ViPNet Coordinator HW/VA-Coordinator

3 Wenn der Zugriff mobiler Apple-Geräte auf geschützte ViPNet Knoten sichergestellt werden soll, öffnen Sie die Registerkarte **Tunnel** und fügen Sie die IP-Adresse 192.168.30.0/24 zur Liste **IP-Adressen der getunnelten Verbindungen** hinzu. Standardmäßig werden Adressen aus diesem Bereich an mobile Geräte vergeben, wenn sich diese Geräte über das IPsec-Protokoll zum ViPNet Coordinator HW/VA verbinden.

4 Klicken Sie in der Navigationsleiste auf **Client hinzufügen** und wahlen Sie im Menü **Client iOS IPsec**.

5 Wenn nötig, benennen Sie den neu hinzugefügten mobilen Client um. Klicken Sie dazu mit der rechten Maustaste auf den Smartphone-Client und wählen Sie im Kontextmenü den Befehl **Umbenennen**.

6 Wählen Sie den hinzugefügten Client in der Navigationsleiste aus. Seine Parameter werden in der Panel-Ansicht angezeigt.

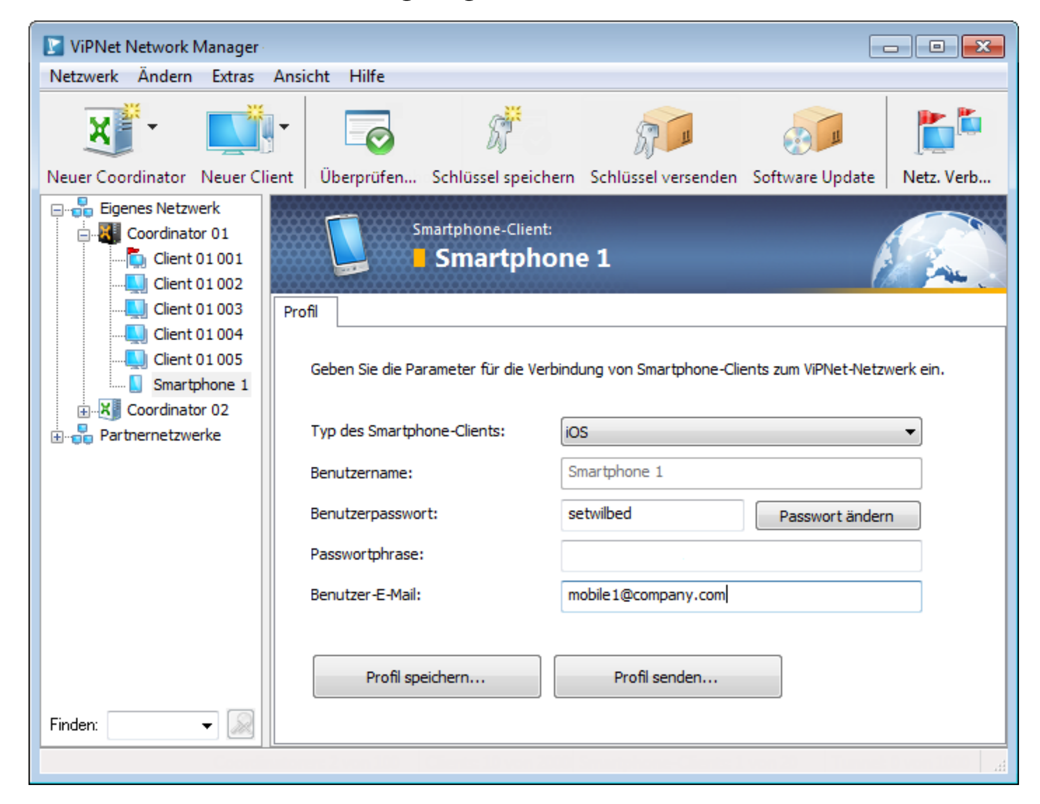


Abbildung 45: Parameter des Smartphone-Clients

7 Klicken Sie zum Festlegen des Passworts, das für die Verbindung zum IPsec-Gateway verwendet werden soll, auf die Schaltfläche **Passwort ändern**. Geben Sie dann im Fenster **Benutzerpasswort** das erforderliche Passwort ein.

Achtung! Der Benutzerpasswort darf die folgenden Zeichen nicht enthalten: Fragezeichen (?), umgekehrter Schrägstrich (\), einfaches Anführungszeichen (‘).

8 Geben Sie im Feld **Benutzer-E-Mail** eine E-Mail-Adresse ein, die dazu verwendet werden kann, die IPsec-Verbindungseinstellungen an das mobile Gerät zu versenden.

9 Klicken Sie auf **Profil senden**. Es wird das Standard-E-Mail-Programm gestartet. In diesem Programm wird automatisch eine neue E-Mail-Nachricht angelegt, die an den Benutzer des mobilen Geräts adressiert ist. Das IPsec-Profil mit den IPsec-Verbindungsparametern wird der Nachricht als Anhang hinzugefügt.

10 Versenden Sie die E-Mail-Nachricht. Sobald der Benutzer des mobilen Geräts die Nachricht erhält, sollte er das empfangene IPsec-Profil auf seinem Gerät anwenden. Weitere Informationen finden Sie im Dokument „ViPNet VPN. Benutzerhandbuch".

11 Wählen Sie in der Navigationsleiste den ViPNet Coordinator HW/VA-Knoten aus, der als IPsec-Gateway auftreten soll. Klicken Sie in der Panel-Ansicht auf der Registerkarte **Schlüssel** auf **Schlüssel senden**, um die IPsec-Verbindungseinstellungen an den ViPNet Coordinator HW/VA-Knoten zu übertragen.

   Wenn noch keine Schlüssel auf dem ViPNet Coordinator HW/VA-Knoten installiert wurden, klicken Sie auf **Schlüssel speichern**, um eine *.dst-Datei zu erstellen. Installieren Sie anschließend diese Schlüssel auf dem ViPNet Coordinator HW/VA-Knoten (s. Installation der Schlüsseldistribution auf S. 37).

Anbindung mobiler Android-Geräte

Damit mobile Android-Geräte auf geschützte Unternehmensressourcen zugreifen können, sollten IPsec-Verbindungseigenschaften in ViPNet Network Manager auf die gleiche Weise wie für Apple-Geräte konfiguriert werden. Der Unterschied besteht darin, dass IPsec-Profile nicht an Android-Geräte versendet werden können. Deswegen sollte das Gerät manuell konfiguriert werden.

Wenn ein Android-Gerät Verbindungen zu geschützten Unternehmensressourcen herstellen soll:

1 Folgen Sie den Schritten 1–7 im Abschnitt Anbindung mobiler Apple-Geräte (auf S. 153).

2 Senden Sie Schlüssel an den ViPNet Coordinator HW/VA-Knoten, der als IPsec-Gateway auftritt, um die IPsec-Verbindungseinstellungen zu übertragen.

3 Fügen Sie ein IPsec-Profil auf Ihrem Android-Gerät hinzu:

   3.1 Klicken Sie auf das Menü **Einstellungen** > **Wireless & Networking** > **VPN**.

   3.2 Erstellen Sie ein neues VPN-Profil.

   3.3 Legen Sie als Verbindungstyp **L2TP/IPSec PSK** fest.

   3.4 Geben Sie zum Festlegen der Serveradresse die IP-Adresse oder den DNS-Namen des ViPNet Coordinator HW/VA-Knotens, die Sie in ViPNet Network Manager definiert haben, auf der Registerkarte **IPsec-Verbindung** (s. Abbildung auf S. 154) ein.

   3.5 Geben Sie zum Festlegen des Pre-Shared Keys den Pre-Shared Key, den Sie auf der Registerkarte **IPsec-Verbindung** angegeben haben, ein.

3.6 Speichern Sie das VPN-Profil.

4 Tippen Sie auf das erstellte VPN-Profil. Die Benutzer-Anmeldeinformationen werden angefordert:

4.1 Geben Sie den Benutzernamen, den Sie in ViPNet Network Manager definiert haben, auf der Eigenschaften-Registerkarte des Smartphone-Clients ein (s. Abbildung auf S. 155).

4.2 Geben Sie das Passwort, das Sie in ViPNet Network Manager definiert haben, auf der Eigenschaften-Registerkarte des Smartphone-Clients ein.

4.3 Tippen Sie auf **Verbinden**.

Hinweis. Die Bezeichnung und Anordnung der aufgelisteten Optionen kann sich auf Ihrem Android-Gerät von der hier genannten unterscheiden. Weitere Informationen finden Sie im Benutzerhandbuch des entsprechenden Geräts.

Bereitstellung des Internetzugangs für mobile Geräte während der IPsec-Sitzungen

Der Internetzugang für mobile IPsec-Clients kann am einfachsten mit Hilfe des integrierten Proxyservers im transparenten Modus auf dem ViPNet Coordinator HW/VA sichergestellt werden (s. Konfiguration des Proxy-Servers auf S. 89). Dazu:

1. Melden Sie sich auf der Webschnittstelle von ViPNet Coordinator HW/VA als Administrator an und gehen Sie zur Proxyserver-Konfigurationsseite.
2. Auf der Registerkarte **Allgemeine**:
   - Wählen Sie in der Liste **Externer Netzwerkadapter** den Adapter aus, der mit dem Internet verbunden ist.
   - Aktivieren Sie das Kontrollkästchen **„Transparenter“ Arbeitsmodus**.
   - Klicken Sie auf **Speichern**.
3. Fügen Sie auf der Registerkarte **Abzuhörende Adressen** alle lokalen IP-Adressen des ViPNet Coordinator HW/VA-Knotens zur Liste hinzu (mit Ausnahme von 127.0.0.1).
4. Fügen Sie auf der Registerkarte **Bediente Netzwerke** die Netzwerk-IP-Adresse 192.168.30.0/24 zur Liste hinzu. Die IP-Adressen aus diesem Bereich werden den mobilen Geräten zugewiesen, die sich über das IPsec-Protokoll mit dem ViPNet Coordinator HW/VA verbinden.
5. Starten Sie auf der Registerkarte **Allgemeine** den Proxyserver.

Statt den Proxyserver zu verwenden, können Sie auch Traffic-Verarbeitungsregeln definieren, die den Zugang mobiler IPsec-Clients zum Internet erlauben:

- eine Transitregel (s. Regeln zur Filterung des Traffics auf S. 112), die den ausgehenden IP-Traffic aus dem Netzwerk 192.168.30.0/24 in Richtung Internet erlaubt;
- eine Regel der Quellübersetzung (s. Regeln der Adressenübersetzung auf S. 114), die IP-Adressen aus dem Netzwerk 192.168.30.0/24 durch die öffentliche IP-Adresse des ViPNet Coordinator HW/VA-Knotens substituiert.

Bereitstellung eines sicheren Zugangs zu Ressourcen im Firmen-LAN aus anderen LANs (Site-to-Site Verbindung)

Bei Firmennetzwerken stellt sich oft die Aufgabe, Traffic, der zwischen zwei entfernten lokalen Netzwerken ausgetauscht wird, effektiv zu schützen.

Wenn die Remotenetzwerke ein- und derselben Firma gehören, dann kann ein geschützter Kanal zwischen diesen Netzwerken mit Hilfe von ViPNet Software organisiert werden. Damit zum Beispiel die Zentrale durch einen abgesicherten Kanal mit einer Filiale verbunden wird, kann in der Filiale ViPNet Coordinator HW/VA installiert werden. Dieses Schema wird im Abschnitt Verbindungen über den geschützten ViPNet Kanal (auf S. 159) beschrieben.

Wenn in einem der entfernten Netzwerke keine ViPNet Technologie verwendet werden kann, dann ist der Schutz des Traffics durch Verschlüsselung nach dem IPsec-Protokoll möglich. In diesem Fall kann ViPNet Coordinator HW/VA die Rolle eines ViPNet IPsec-Gateways übernehmen. Dieses Schema wird im Abschnitt Verbindungen über einen geschützten IPsec-Kanal (auf S. 161) beschrieben.

Verbindungen über den geschützten ViPNet Kanal

Nehmen wir an: im Hauptstandort eines Unternehmens ist ein geschütztes ViPNet VPN-Netzwerk eingerichtet und es soll eine sichere Verbindung mit einer Filiale hergestellt werden. In der Filiale sind sowohl geschützte ViPNet als auch getunnelte Netzwerkknoten vorhanden.

So wird eine solche Verbindung hergestellt:

- In der Hauptniederlassung sollte ein Coordinator eingerichtet werden, der über eine statische IP-Adresse oder einen festen DNS-Namen aus dem Internet erreichbar ist.
- Ein ViPNet Coordinator HW/VA-Knoten sollte an der Grenze des lokalen Netzwerks der Niederlassung installiert werden. Dieser soll als eine Firewall für ViPNet Knoten auftreten und die ungeschützten Knoten im LAN tunneln.

  Der Coordinator sollte mit dem Internet verbunden sein, um auf das Hauptsitz-VPN zuzugreifen. Es ist jedoch nicht erforderlich, dass der Coordinator selbst aus dem Hauptsitz-VPN erreichbar ist (er kann z. B. eine dynamische IP-Adresse verwenden).

Obwohl sich der Begriff „Site-to-Site Verbindung“ im Allgemeinen auf die Tunnelung von Verbindungen zwischen den Knoten im LAN und dem Hauptsitz-VPN bezieht, kann das LAN der Zweigniederlassung zusätzlich ViPNet Clients enthalten, die ebenfalls eine Verbindung zum Hauptsitz-VPN aufbauen können. Im folgenden Beispiel enthält das LAN der Zweigniederlassung sowohl getunnelte Knoten als auch ViPNet Clients.

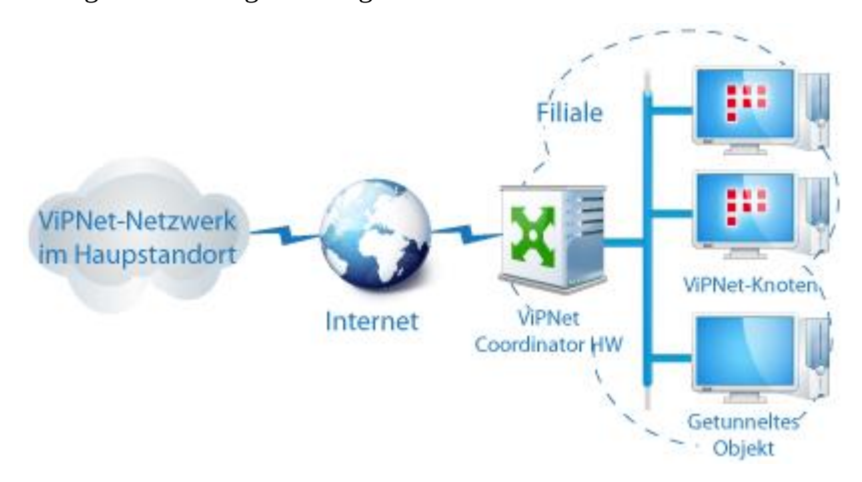


Abbildung 46: Verwendung des ViPNet Coordinator HW/VA zur Verbindung von zwei voneinander entfernten Standorten

Gehen Sie wie folgt vor, um eine verschlüsselte Verbindung mit der Zweigniederlassung über einen geschützten Tunnel aufzubauen:

1 Richten Sie einen ViPNet Coordinator HW/VA-Knoten im LAN der Niederlassung ein (s. Vorgehensweise bei der Installation von ViPNet Coordinator HW/VA auf S. 29). Beachten Sie dabei Folgendes:

1.1 Stellen Sie sicher, dass Sie vom Coordinator der Zweigniederlassung auf den Coordinator des Hauptsitzes über das Internet unter Verwendung seiner IP-Adressen und DNS-Namen zugreifen können.

1.2 Gehen Sie beim Konfigurieren des ViPNet Coordinator HW/VA-Knotens im ViPNet Network Manager (s. Konfiguration der Netzwerkeinstellungen von ViPNet Coordinator HW/VA in ViPNet Network Manager auf S. 62) wie folgt vor:

- Fügen Sie die ViPNet Clients der Niederlassung dem neuen Coordinator hinzu.
- Legen Sie die IP-Adressen des ViPNet Coordinator HW/VA auf der Registerkarte **IP-Adressen** fest.
- Definieren Sie abhängig vom Internet-Verbindungstyp des ViPNet Coordinator HW/VA-Knotens die Firewallparameter auf der Registerkarte **Firewall**.

Hinweis. In den meisten Fällen wird ein Internetzugang bereitgestellt, wenn der Firewall-Typ **Mit dynamischem NAT** gewählt wird. Als **Coordinator für eingehende Verbindungen** sollte der vom Internet zugängliche Coordinator am Hauptstandort eingetragen werden.

- Wenn der ViPNet Coordinator HW/VA einen offenen Netzwerkknoten der Filiale tunneln soll, geben Sie die entsprechenden Parameter in der Registerkarte **Tunnelung** ein.

2 Wenn ViPNet Clients im LAN der Zweigniederlassung installiert werden sollen, dann richten Sie diese nun ein. Stellen Sie dabei sicher, dass für jeden Client im ViPNet Network Manager die folgenden Parameter eingestellt sind:

- o der ViPNet Coordinator HW/VA-Coordinator ist als IP-Adressenserver (VPN-Server) festgelegt;
- o die Optionen der Clientfirewall sind korrekt konfiguriert.

Weitere Informationen finden Sie im Dokument „ViPNet VPN. Benutzerhandbuch".

3 Sollen im LAN der Zweigniederlassung getunnelte Knoten erreicht werden, so führen Sie eine der folgenden Aktionen auf den zu tunnelnden Knoten durch:

- o Als Standardgateway tragen Sie das ViPNet Coordinator HW/VA ein.
- o Geben Sie die statische Route an, damit der getunnelte Netzwerkknoten den zum verschlüsselnl bestimmten Datenverkehr über das ViPNet Coordinator HW/VA sendet.

  Führen Sie zum Beispiel auf einem getunnelten Knoten mit dem Betriebssystem Windows in der Kommandozeile den folgenden Befehl aus:

```
route add <IP-Zieladresse> mask <Subnetzmaske> <IP-Adresse von ViPNet
Coordinator HW/VA> -p
```

4 Wenn alle Einstellungen richtig sind, wird zwischen den Standorten eine geschützte Verbindung eingerichtet. Um dies zu überprüfen, stellen Sie eine Verbindung zwischen den Clients in der Zweigniederlassung und dem Hauptsitz her.

Verbindungen über einen geschützten IPsec-Kanal

Nehmen wir an, dass Ihr Firmennetzwerk durch ein ViPNet VPN geschützt ist. Sie möchten einen abgesicherten Kanal für die Kommunikation mit einer Partnerfirma einrichten, die keine ViPNet Technologie verwendet.

In diesem Fall kann ein Tunnel zwischen den zwei unternehmensinternen Netzwerken unter Verwendung des IPsec-Protokolls eingerichtet werden. Ein IPsec-Tunnel ist ein verschlüsselter

Traffic-Tunnel zwischen zwei IPsec-Gateways (ein IPsec-Gateway befindet sich in jedem der zwei Netzwerke). Es steht eine Vielzahl an IPsec-Gateway Softwareservern und Geräten zur Verfügung (Cisco-Geräte, Server mit Linux, FreeBSD, Windows-Server, u. s. w.).

Ein ViPNet Coordinator HW/VA-Knoten kann ebenfalls als das IPsec-Gateway Ihres Netzwerks verwendet werden.

Achtung! Es können keine geschützten IPsec-Kanäle zwischen zwei ViPNet Coordinator HW/VA-Knoten eingerichtet werden, die zum gleichen ViPNet Netzwerk gehören. Der Tunnel kann aber für Knoten eingerichtet werden, die sich im Partnernetzwerk befinden (weitere Details s. Dokument „ViPNet VPN. Benutzerhandbuch“, Kapitel „Aufbau der Verbindung zum Partnernetzwerk“).

Beachten Sie das folgende Beispiel:

Abbildung 47: Aufbau von Verbindungen über das IPsec-Protokoll

Der Knoten des Remotenetzwerks 10.0.0.2 baut eine Verbindung zum Knoten 172.16.0.2 im ViPNet Netzwerk auf. Dabei werden die IP-Pakete des Knotens 10.0.0.2 offen zum Gerät „Remote Gate“ übertragen. Auf diesem Gerät wird die Verschlüsselung der IP-Pakete und die Übersetzung der Absender-IP-Adresse in die externe Geräteadresse 87.142.218.3 durchgeführt. Anschließend führt ViPNet Coordinator HW/VA die umgekehrte Aktion durch und leitet die Pakete in ihrem Originalzustand an den Knoten 172.16.0.2 weiter.

Damit IPsec-Verbindungen konfiguriert werden können, sollten auf Remote Gate-Geräten und in ViPNet Coordinator HW/VA die IP-Adressen der interagierenden Netzwerke, die eigenen Geräteadressen, das Verschlüsselungsprotokoll und der Modus der Anmeldung untereinander abgestimmt werden.

In ViPNet Network Manager kann eine IPsec-Verbindung mit Authentifizierung auf Basis eines Pre-Shared Keys (PSK) konfiguriert werden. Wenn Sie Zertifikatsauthentifizierung verwenden möchten, finden Sie die Informationen dazu im Dokument „ViPNet Coordinator HW/VA. Referenzhandbuch“.

Gehen Sie wie folgt vor, um eine standortübergreifende IPsec-Verbindung (Site-to-Site) im ViPNet Network Manager zu konfigurieren:

1 Wählen Sie in der Navigationsleiste den ViPNet Coordinator HW/VA-Knoten aus, der als IPsec-Gateway auftreten soll.

Achtung! Wenn Sie auf dem ViPNet Coordinator HW/VA-Knoten noch keine Schlüsseldistribution installiert haben und eine automatische Schlüsselinstallation durchführen möchten (s. Automatische Installation der Schlüsseldistribution auf S. 38), dann sollten Sie die IPsec-Verbindungseinstellungen erst nach der erfolgten Installation der Schlüssel konfigurieren.

2 Klicken Sie in der Panel-Ansicht auf die Registerkarte **IPsec-Verbindung**.

3 Wenn Sie ViPNet Coordinator HW/VA noch nie zuvor als IPsec-Gateway eingerichtet haben, gehen Sie folgendermaßen vor:

3.1 Wählen Sie in der Liste **Netzwerkadapter-Name** den Netzwerkadapter auf dem ViPNet Coordinator HW/VA-Knoten aus, der aus dem Internet angesprochen werden kann.

3.2 Aktivieren Sie das Kontrollkästchen **Coordinator für geschützte IPsec-Verbindungen anderer Netzwerke verwenden**.

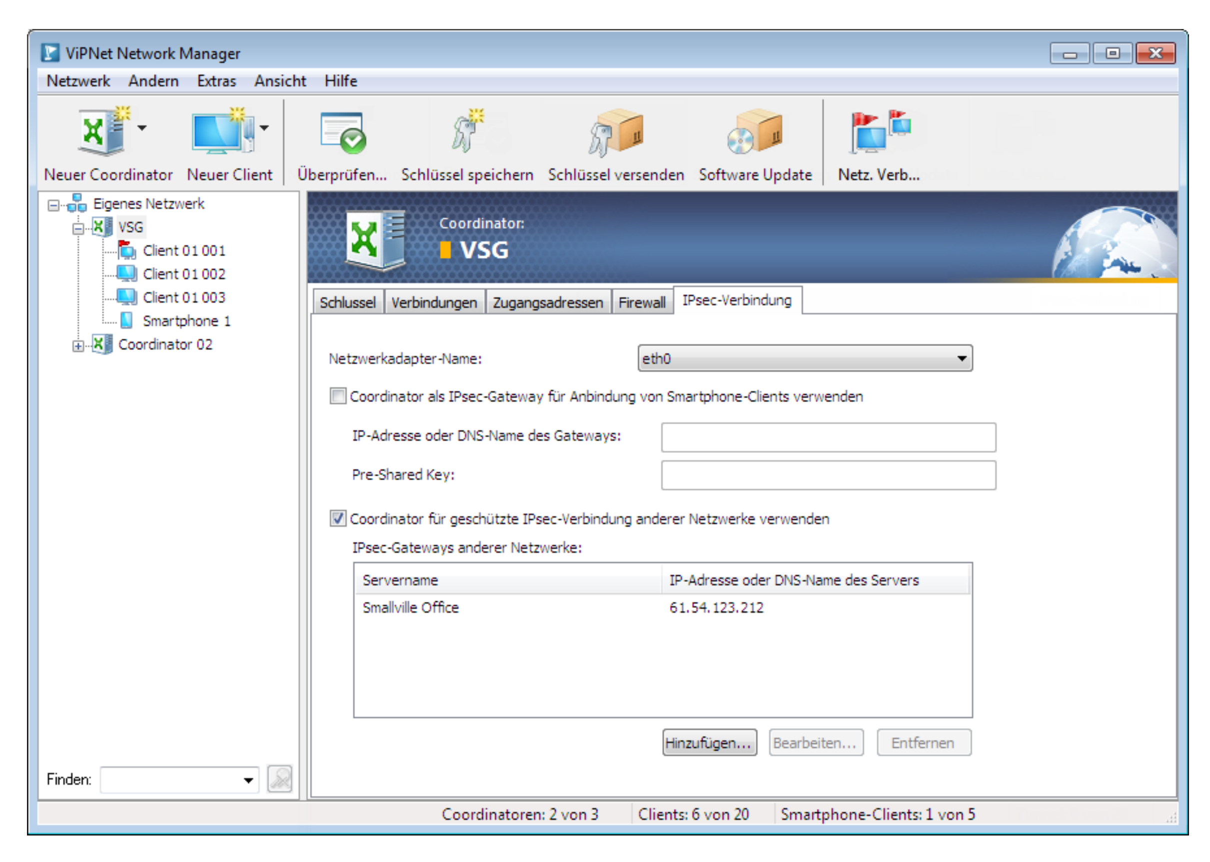


Abbildung 48: Hinzufügen eines IPsec-Kanals zu einem anderen Netzwerk

4 Klicken Sie auf **Hinzufügen**, um einen neuen IPsec-Kanal zum Remotenetzwerk zu konfigurieren. Das Fenster **IPsec-Gateway Neu** wird geöffnet.

5 Geben Sie auf der Registerkarte **Verbindung** im Feld **Remotegateway-Name** einen eindeutigen Namen für die Verbindung zum Remotenetzwerk an.

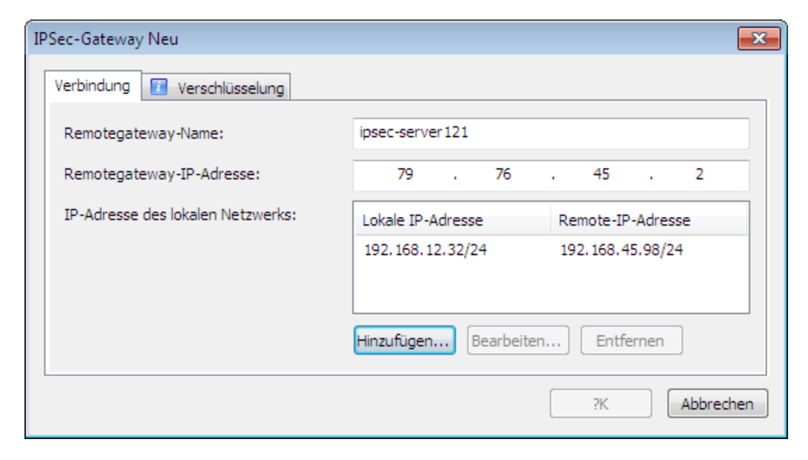


Abbildung 49: Ahgeben der Parameter für remote IPsec-Gateway

6 Geben Sie im Feld **Remotegateway-IP-Adresse** die Zugangsadresse des entfernten IPsec-Gateways an.

7 Klicken Sie auf **Hinzufügen**. Definieren Sie im Fenster **Adressen des lokalen und Remotenetzwerks** die IP-Adressen der Netzwerke, die mittels IPsec-Kanal miteinander verbunden werden sollen. Netzwerkadressen sollten in der CIDR-Notation angegeben werden, zum Beispiel 172.16.0.0/24.

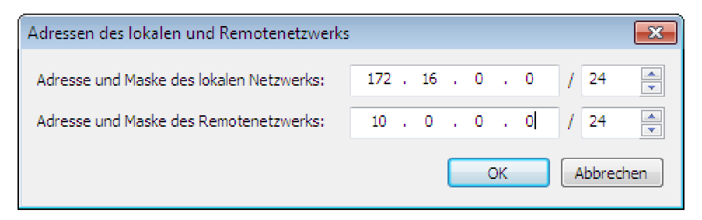


Abbildung 50: Festlegen des lokalen und Remotenetzwerks

Wenn nötig, wiederholen Sie diesen Schritt, um weitere Paare von lokalen und Remotenetzwerken zu erstellen.

8 Öffnen Sie die Registerkarte Verschlüsselung und konfigurieren Sie die Verschlüsselungsparameter der Verbindung:

- Geben Sie im Feld **Pre-Shared Key** eine beliebige Reihenfolge an Zeichen ein (8 bis 63 Zeichen lang). Diese Zeichenfolge wird als Passwort für die Verbindungsauthentifizierung verwendet.

Achtung! Der Pre-Shared Key darf die folgenden Zeichen nicht enthalten: Fragezeichen (?), umgekehrter Schrägstrich (\), einfaches Anführungszeichen (‘).

- Wenn nötig, geben Sie den Verschlüsselungs- und Hashalgorithmus, den Diffie-Hellman-Parameter und die Gültigkeitsdauer der Schlüssel in den entsprechenden Feldern an.

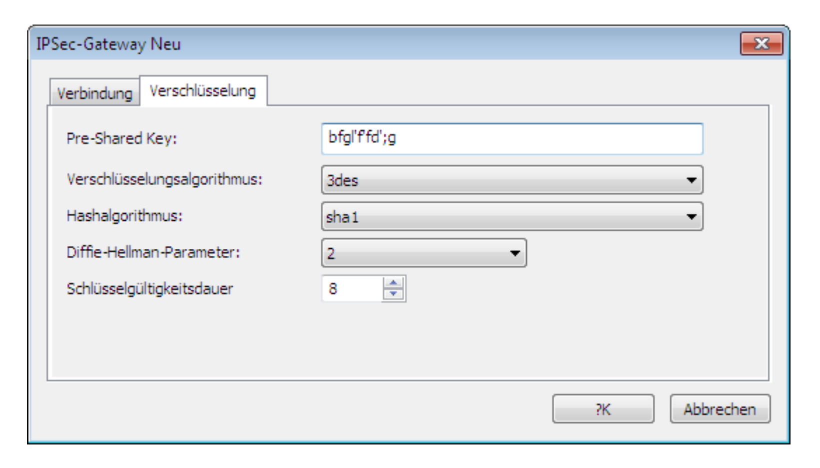


Abbildung 51: Definition der Verschlüsselungsparameter

Achtung! Informieren Sie den Administrator des Remotenetzwerks, dass die gleichen Verschlüsselungsparameter auf dem Remotegateway eingestellt werden sollen.

9 Klicken Sie in der Panel-Ansicht auf der Registerkarte **Schlüssel** auf **Schlüssel senden**, um die IPsec-Verbindungseinstellungen an den ViPNet Coordinator HW/VA-Knoten zu übertragen.

Wenn noch keine Schlüssel auf dem ViPNet Coordinator HW/VA-Knoten installiert wurden, klicken Sie auf **Schlüssel speichern**, um eine `*.dst`-Datei zu erstellen. Installieren Sie dann diese Schlüssel auf dem ViPNet Coordinator HW/VA-Knoten (s. Installation der Schlüsseldistribution auf S. 37).

10 Konfigurieren Sie auf dem ViPNet Coordinator HW/VA-Knoten eine Transitregel, die den Traffic zwischen dem Remotenetzwerk und dem lokalen Netzwerk, das Sie in ViPNet Network Manager definiert haben, erlaubt.

Hinweis. Wenn Sie möchten, dass die Computer des Remotenetzwerks auf geschützte ViPNet Knoten im lokalen Netzwerk zugreifen können, dann sollten Sie Firewall-Regeln auf den lokalen Knoten definieren, die den eingehenden Traffic der Remoteknoten erlauben.

Manuelle Konfiguration der integrierten Firewall für den Zugruiff des Netzwerkknoten ins Internet aus lokalem Netzwerk

Wenn Sie einen 3G/LTE-Internetzugang über die Appliance einstellen, dann sollten Sie zusätzlich die integrierte Firewall konfigurieren (s. Konfiguration der integrierten Firewall auf S. 105), damit Knoten, die sich hinter einem Coordinator befinden, auf das Internet zugreifen können.

Wenn Ihre Coordinator HW-Plattform keine Proxyserver-Funktionalität unterstützt, dann sollten Sie die Firewall manuell unter Verwendung der Befehlszeilenschnittstelle konfigurieren (s. Verwalten von ViPNet Coordinator HW/VA-Knoten auf S. 46). Gehen Sie wie folgt vor:

1. Wechseln Sie in der Befehlszeilenschnittstelle in den Administratormodus, indem Sie den Befehl enable ausführen.
2. Stopen Sie den ViPNet Treiber, indem Sie den Befehl `iplir stop` ausführen.
3. Öffnen Sie die Konfigurationsdatei der Firewall, indem Sie den Befehl `iplir config firewall` ausführen.

4 Fügen Sie im Bereich `[nat]` eine NAT-Regel für Verbindungen lokaler Knoten mit dem Internet hinzu. Wenn das lokale Netzwerk z. B. die Adresse `192.168.125.0/24` besitzt, dann fügen Sie die folgende Regel hinzu:

```
rule = num [X] proto any from 192.168.125.0/24 to internet change
src=modem:dynamic
```

wobei `<interface>` kann folgende Werte aufnehmen:

- wenn Sie eine 3G/LTE-Verbindung konfigurieren: `modem`
- wenn Sie eine Wi-Fi-Verbindung konfigurieren: `wlan0`
- wenn Sie eine Ethernet-Verbindung konfigurieren: eth<X> (Netzwerkadapter des öffentlichen Netzwerks)

5 Fügen Sie im Bereich `[forward]` eine Regel hinzu, die Verbindungen lokaler Knoten zum Internet erlaubt. Beispiel:

```
rule = num [X] proto any from 192.168.125.0/24 to anyip pass
```

6 Speichern Sie die Einstellungen und beenden Sie die Konfiguration durch Drücken von **Strg+X**.

7 Starten Sie den ViPNet Treiber, indem Sie den Befehl `iplir start` ausführen.

Information zu Drittanbieter-Softwarekomponenten

Während der Anwendungsentwicklung wurden Softwarekomponenten einiger Drittanbieter eingesetzt. Die Verbreitung und Nutzung dieser Komponenten unterliegt den Bestimmungen der jeweiligen Lizenzvereinbarungen. Die Texte dieser Lizenzvereinbarungen sind weiter unten aufgeführt.

Innerhalb von mindestens drei Jahren ab dem Vertriebszeitpunkt des zutreffenden Produkts oder Software stellen wir jedem, der sich an uns in dieser Angelegenheit wendet, eine vollständige maschinenlesbare Kopie des kompletten Quellcodes derjenigen Version des Programms, die an den Anfragenden verkauft wurde, bereit (vorausgesetzt, dieser Quellcode steht uns zur Verfügung). Dafür wird ein Entgelt verrechnet, der die Kosten der physikalischen Bereitstellung des Quellcodes unsererseits deckt.

Apache

Apache License, Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/ http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

License shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

Licensor shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

Legal Entity shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, control means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

You (or Your) shall mean an individual or Legal Entity exercising permissions granted by this License.

Source form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

Object form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

Work shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

Derivative Works shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

Contribution shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, submitted means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as Not a Contribution.

Contributor shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a NOTICE text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an AS IS BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets [] replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same printed page as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]
Licensed under the Apache License, Version 2.0 (the License);
you may not use this file except in compliance with the License.
You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an AS IS BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and

limitations under the License.

Busybox

Mail all comments, insults, suggestions and bribes to

Denys Vlasenko vda.linux@googlemail.com vda.linux@googlemail.com

BusyBox is licensed under the GNU General Public License version 2, which is often abbreviated as GPLv2.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if

you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The Program, below, refers to any such program or work, and a work based on the Program means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term modification.) Each licensee is addressed as you.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an

appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and any later version, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving

the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the copyright line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author
```

```
This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free Software
Foundation; either version 2 of the License, or (at your option) any later
version.

This program is distributed in the hope that it will be useful, but WITHOUT
ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS
FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with
this program; if not, write to the Free Software Foundation, Inc., 51 Franklin
Street, Fifth Floor, Boston, MA 02110-1301, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author Gnomovision comes
with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software,
and you are welcome to redistribute it under certain conditions; type 'show c'
for details.
```

The hypothetical commands '`show w`' and '`show c`' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than '`show w`' and '`show c`'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a copyright disclaimer for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License http://www.gnu.org/licenses/lgpl.html instead of this License.

Editline Library (libedit)

Some files are:

This code is derived from software contributed to Berkeley by Christos Zoulas of Cornell University.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some files are:

This code is derived from software contributed to The NetBSD Foundation by Anthony Mallet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some files are:

This code is derived from software contributed to The NetBSD Foundation by Jaromir Dolecek.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some files are:

Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED AS IS AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

ICU

ICU License - ICU 1.8.1 and later

IPsec-Tools

Libclamav

Libclamav is licensed under the GNU General Public License version 2, which is often abbreviated as GPLv2.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The Program, below, refers to any such program or work, and a work based on the Program means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term modification.) Each licensee is addressed as you.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through

you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and any later version, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the copyright line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author


This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free Software
Foundation; either version 2 of the License, or (at your option) any later
version.
```

```
This program is distributed in the hope that it will be useful, but WITHOUT
ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS
FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with
this program; if not, write to the Free Software Foundation, Inc., 51 Franklin
Street, Fifth Floor, Boston, MA 02110-1301, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author Gnomovision comes
with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software,
and you are welcome to redistribute it under certain conditions; type 'show c'
for details.
```

The hypothetical commands '`show w`' and '`show c`' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than '`show w`' and '`show c`'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a copyright disclaimer for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License http://www.gnu.org/licenses/lgpl.html instead of this License.

libxml2

Some files are:

Some files are:

Some files are:

Author: breese@users.sourceforge.net

Some files are:

Author: Gary.Pennington@uk.sun.com

MD5

MD5.H

MD5.H

License to copy and use this software is granted provided that it is identified as the RSA Data Security, Inc. MD5 Message-Digest Algorithm in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided as is without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

MD5-CC 1.02

This software contains a C++/object oriented translation and modification of MD5 (version 1.02) by Mordechai T. Abzug. Translation and modification (c) 1995 by Mordechai T. Abzug

Copyright 1991-1992 RSA Data Security, Inc.

The MD5 algorithm is defined in RFC 1321. This implementation is derived from the reference C code in RFC 1321 which is covered by the following copyright statement:

Nano 1.3.7

Nano 1.3.7 is licensed under the GNU General Public License version 2, which is often abbreviated as GPLv2.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free

software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The Program, below, refers to any such program or work, and a work based on the Program means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term modification.) Each licensee is addressed as you.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and any later version, you have the option of following the terms and conditions either of that version or of any later version published by the

Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the copyright line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author


This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free Software
Foundation; either version 2 of the License, or (at your option) any later
version.

This program is distributed in the hope that it will be useful, but WITHOUT
ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS
FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with
this program; if not, write to the Free Software Foundation, Inc., 51 Franklin
Street, Fifth Floor, Boston, MA 02110-1301, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author Gnomovision comes
with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software,
and you are welcome to redistribute it under certain conditions; type 'show c'
for details.
```

The hypothetical commands '`show w`' and '`show c`' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than '`show w`' and '`show c`'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a copyright disclaimer for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.
```

```
signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License http://www.gnu.org/licenses/lgpl.html instead of this License.

STLport

License Agreement

Boris Fomitchev grants **Licensee** a non-exclusive, non-transferable, royalty-free license to use **STLport** and its documentation without fee.

By downloading, using, or copying **STLport** or any portion thereof, **Licensee** agrees to abide by the intellectual property laws and all other applicable laws of the United States of America, and to all of the terms and conditions of this Agreement.

Licensee shall maintain the following copyright and permission notices on **STLport** sources and its documentation unchanged:

Copyright 1999,2000 Boris Fomitchev

This material is provided as is, with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

The **Licensee** may distribute binaries compiled with **STLport** (whether original or modified) without any royalties or restrictions.

The **Licensee** may distribute original or modified **STLport** sources, provided that:

The conditions indicated in the above permission notice are met;

The following copyright notices are retained when present, and conditions provided in accompanying permission notices are met :

Copyright 1994 Hewlett-Packard Company

Copyright 1996,97 Silicon Graphics Computer Systems, Inc.

Copyright 1997 Moscow Center for SPARC Technology.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all

copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided as is without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided as is without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Moscow Center for SPARC Technology makes no representations about the suitability of this software for any purpose. It is provided as is without express or implied warranty.

SQLite

SQLite Copyright

SQLite is in the Public Domain http://en.wikipedia.org/wiki/Public_Domain

All of the deliverable code in SQLite has been dedicated to the public domain by the authors. All code authors, and representatives of the companies they work for, have signed affidavits dedicating their contributions to the public domain and originals of those signed affidavits are stored in a firesafe at the main offices of Hwaci. Anyone is free to copy, modify, publish, use, compile, sell, or distribute the original SQLite code, either in source code form or as a compiled binary, for any purpose, commercial or non-commercial, and by any means.

The previous paragraph applies to the deliverable code in SQLite - those parts of the SQLite library that you actually bundle and ship with a larger application. Portions of the documentation and some code used as part of the build process might fall under other licenses. The details here are unclear. We do not worry about the licensing of the documentation and build code so much because none of these things are part of the core deliverable SQLite library.

All of the deliverable code in SQLite has been written from scratch. No code has been taken from other projects or from the open internet. Every line of code can be traced back to its original author, and all of those authors have public domain dedications on file. So the SQLite code base is clean and is uncontaminated with licensed code from other projects.

Obtaining An Explicit License To Use SQLite

Even though SQLite is in the public domain and does not require a license, some users want to obtain a license anyway. Some reasons for obtaining a license include:

You are using SQLite in a jurisdiction that does not recognize the public domain.

You are using SQLite in a jurisdiction that does not recognize the right of an author to dedicate their work to the public domain.

You want to hold a tangible legal document as evidence that you have the legal right to use and distribute SQLite.

Your legal department tells you that you have to purchase a license.

If you feel like you really have to purchase a license for SQLite, Hwaci http://www.hwaci.com/, the company that employs the architect and principal developers of SQLite, will sell you one http://www.hwaci.com/cgi-bin/license-step1.

Contributed Code

In order to keep SQLite completely free and unencumbered by copyright, all new contributors to the SQLite code base are asked to dedicate their contributions to the public domain. If you want to send a patch or enhancement for possible inclusion in the SQLite source tree, please accompany the patch with the following statement:

The author or authors of this code dedicate any and all copyright interest in this code to the public domain. We make this dedication for the benefit of the public at large and to the detriment of our heirs and successors. We intend this dedication to be an overt act of relinquishment in perpetuity of all present and future rights to this code under copyright law.

We are not able to accept patches or changes to SQLite that are not accompanied by a statement such as the above. In addition, if you make changes or enhancements as an employee, then a simple statement such as the above is insufficient. You must also send by surface mail a copyright release signed by a company officer. A signed original of the copyright release should be mailed to:

Hwaci

6200 Maple Cove Lane

Charlotte, NC 28269

USA

A template copyright release is available in PDF http://www.sqlite.org/copyright-release.pdf or HTML http://www.sqlite.org/copyright-release.html. You can use this release to make future changes.

Squid

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (version 2) as published by the Free Software Foundation. It is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Squid is licensed under the GNU General Public License version 2, which is often abbreviated as GPLv2.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if

you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The Program, below, refers to any such program or work, and a work based on the Program means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term modification.) Each licensee is addressed as you.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an

appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and any later version, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving

the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the copyright line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author
```

```
This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free Software
Foundation; either version 2 of the License, or (at your option) any later
version.

This program is distributed in the hope that it will be useful, but WITHOUT
ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS
FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with
this program; if not, write to the Free Software Foundation, Inc., 51 Franklin
Street, Fifth Floor, Boston, MA 02110-1301, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author Gnomovision comes
with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software,
and you are welcome to redistribute it under certain conditions; type 'show c'
for details.
```

The hypothetical commands '`show w`' and '`show c`' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than '`show w`' and '`show c`'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a copyright disclaimer for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License http://www.gnu.org/licenses/lgpl.html instead of this License.

sysklogd

This file is part of the sysklogd package, a kernel and system log daemon.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Sysklogd is licensed under the GNU General Public License version 2, which is often abbreviated as GPLv2.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The Program, below, refers to any such program or work, and a work based on the Program means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term modification.) Each licensee is addressed as you.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and any later version, you have the option of following the terms and conditions either of that version or of any later version published by the

Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the copyright line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author


This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free Software
Foundation; either version 2 of the License, or (at your option) any later
version.

This program is distributed in the hope that it will be useful, but WITHOUT
ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS
FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with
this program; if not, write to the Free Software Foundation, Inc., 51 Franklin
Street, Fifth Floor, Boston, MA 02110-1301, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author Gnomovision comes
with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software,
and you are welcome to redistribute it under certain conditions; type 'show c'
for details.
```

The hypothetical commands '`show w`' and '`show c`' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than '`show w`' and '`show c`'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a copyright disclaimer for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.
```

```
signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License http://www.gnu.org/licenses/lgpl.html instead of this License.

UCD-SNMP

License

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF

MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. (Apple) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Xerces-c

Apache License, Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/ http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

License shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

Licensor shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

Legal Entity shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, control means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

You (or Your) shall mean an individual or Legal Entity exercising permissions granted by this License.

Source form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

Object form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

Work shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

Derivative Works shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

Contribution shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, submitted means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as Not a Contribution.

Contributor shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a NOTICE text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an AS IS BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets [] replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same printed page as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]
Licensed under the Apache License, Version 2.0 (the License);
you may not use this file except in compliance with the License.
You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an AS IS BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and

limitations under the License.

zlib

License

Versionsgeschichte

In dieser Anwendung werden die wichtigsten Änderungen in den vorherigen Versionen von ViPNet Coordinator HW/VA beschrieben.

Neu in Version 3.2

Dieser Abschnitt beschreibt neue Möglichkeiten in der Funktionsweise der Software ViPNet Coordinator HW/VA Version 3.2.

- **Failover-System**

  Auf Coordinator VA-Plattformen können Sie nun ein Cluster bereitstellen, das die Funktionen eines eigenständigen Servers erfüllt, sich jedoch deutlich robuster gegenüber Ausfällen verhält. Ein Failover-Cluster besteht aus zwei Knoten mit installiertem Appliance ViPNet Coordinator HW/VA, die ihre Funktionen gegenseitig duplizieren. Das Cluster bleibt funktionsfähig, solange zumindest einer dieser Knoten aktiv ist.

  Die Arbeit mit dem Failover-System wird in einem separaten Dokument „ViPNet Coordinator HW/VA. Failover-System" detailliert beschrieben. Dieses Dokument ist ein Bestandteil des Lieferumfangs (s. Lieferumfang auf S. 16).

- **Stabiler Zugang zu Netzwerkressourcen durch Verwendung alternativer Kanäle**

  Sie können für einen ViPNet Coordinator HW/VA den unterbrechungsfreien Zugang zu einer Netzwerkressource (z. B. Internet) gewährleisten, indem Sie die entsprechende Verbindung über zwei Kanäle herstellen. Sie können dann die Datenverkehrslast auf die zwei Kanäle aufteilen oder den Kanalwechselmodus aktivieren, um den Traffic im Falle eines Kanalausfalls über den jeweils anderen Kanal weiterzuleiten.

- **Konfiguration der ViPNet Coordinator HW/VA-Netzwerkparameter unter Verwendung der Software ViPNet Network Manager**

  Die Netzwerkparameter von ViPNet Coordinator HW/VA einschließlich der Netzwerkadapter- und Routingeinstellungen können nun im Programm ViPNet Network Manager konfiguriert werden.

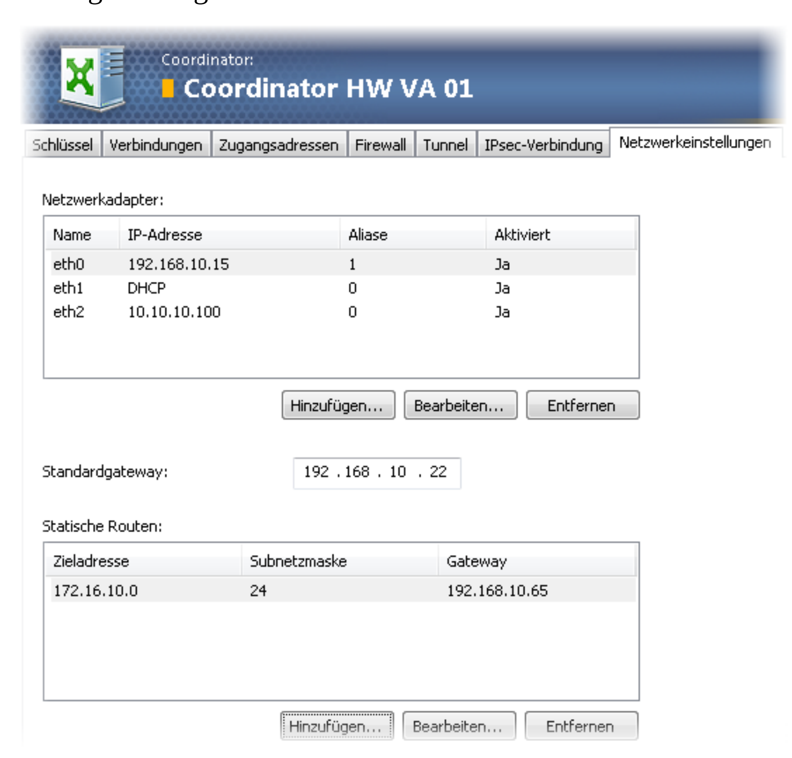
  

  Abbildung 52: Konfiguration der ViPNet Coordinator HW/VA-Netzwerkparameter im ViPNet Network Manager

- **Konfiguration des 3G/LTE-Modems über die Webschnittstelle**

  Nun können Sie die Verbindung über das 3G/LTE-Modem über die Webschnittstelle der Appliance konfigurieren und aktivieren.

- **Folgende 3G/LTE USB-Modems werden unterstützt:**
  - 3G Huawei K3772 (Vodafone),
  - 3G Huawei E303 (Vodafone),
  - LTE Huawei E398 (Deutsche Telekom Speedstick LTE III).

- **ViPNet Coordinator VA unterstützt zusätzliche Festplattenspeicher**

  Jetzt kann eine virtuelle Appliance zusätzliche 80 GB Festplatte zu nutzen. Dies ermöglicht es der Appliance, größere Netzwerke zu bedienen.

- **Konfigurieren der Firewall ist flexibler und einfacher**

  Die NAT-Regeln akzeptieren jetzt Netzwerkadapter-Namen als Argumente (einschließlich der Modem-Netzwerkadapter). Dies vereinfacht die Festlegung der Regeln für Schnittstellen mit dynamischen IP-Adressen.

  Das neue Token `internet` gibt alle Adressen des öffentlichen Adressraum gemeinsam.

- **Installation der Schlüsseldistribution von einer CD**

  Die Schlüssel können nun mit Hilfe einer CD vom ViPNet Network Manager-Knoten an Ihren ViPNet Coordinator HW/VA-Server weitergeleitet werden.

- **Namen von ViPNet VPN-Komponenten haben sich geändert**

  Neben anderen Änderungen:

  - Die ViPNet Security Gateway-Software heißt jetzt ViPNet Coordinator HW/VA.
  - Das ViPNet Manager-Programm heißt jetzt ViPNet Network Manager.

Neu in Version 3.1

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.1 geboten.

- **Webschnittstelle**

  Es wurde eine neue Weboberfläche implementiert, über die Sie die wichtigsten Einstellungen der ViPNet Coordinator HW/VA-Software konfigurieren können.

Abbildung 53: Webschnittstelle von ViPNet Coordinator HW/VA

- **Unterstützung von IPsec-Verbindungen “Client-to-Site“**

  ViPNet Coordinator HW/VA kann nun so konfiguriert werden, dass es als IPsec-Gateway für Client-to-Site-Verbindungen auftritt. Dadurch können Benutzer mit Hilfe ihrer mobilen Geräte über einen abgesicherten IPsec-Kanal auf die Unternehmensressourcen zugreifen.

- **Unterstützung der IPsec-Zertifikatsauthentifizierung**

  Zertifikatsauthentifizierung (RSA) kann nun für IPsec Site-to-Site- und Client-to-Site-Verbindungen konfiguriert werden.

- **Remotekonfiguration von IPsec in ViPNet Network Manager**

  ViPNet Coordinator HW/VA kann nun in ViPNet Network Manager als IPsec-Gateway für Site-to-Site und Client-to-Site-Verbindungen konfiguriert werden. Die Einstellungen werden übernommen, sobald Schlüssel an den ViPNet Coordinator HW/VA-Knoten versendet werden.

- **Automatische Installation der Schlüsseldistribution**

  Für eine automatische Installation der Schlüsseldistribution vom USB-Datenträger auf den ViPNet Coordinator HW/VA-Knoten kann nun die in ViPNet Network Manager generierte Konfigurationsdatei `hwinit_set.xml` verwendet werden.

Neu in Version 3.0

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.0 geboten.

- **Neue ViPNet Treiberarchitektur**

  Es wird die neue, skalierbare Treiberarchitektur von ViPNet angewendet, die zu einer wesentlichen Erhöhung der Leistungsfähigkeit der Verarbeitung des verschlüsselten Traffics insbesondere auf Mehrkernsystemen führt.

- **Unterstützung des VoIP-Servers**

  In ViPNet Coordinator HW/VA-Software wurde ein VoIP-Server integriert, mit dessen Hilfe ein firmeninternes IP-Telefoniesystem aufgebaut werden kann.

- **Unterstützung des Antivirenprogramms „Clam Antivirus“**

  Neben „Kaspersky Antivirus“ wird nun auch das Antivirusprogramm „Clam Antivirus“ unterstützt. Für die Antivirus-Prüfung des Inhalts auf dem Proxyserver kann eines dieser beiden Programme verwendet werden.

- **Möglichkeit zur Verwendung von Auslagerungsdateien**

Das für Software verfügbare Speichervolumen kann nun mit Hilfe einer Auslagerungsdatei vergrößert werden.

Neu in Version 2.3

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 2.3 geboten.

- **Unterstützung von Caching-Proxyserver**

  Im Programmpaket von ViPNet Coordinator HW/VA ist nun ein Proxyserver inkludiert, der im transparenten Modus arbeiten und die Inhalts- und Antiviruskontrolle durchführen kann.

- **Remote-Administration von ViPNet Coordinator HW/VA mit Hilfe des Applets ViPNet SGA**

  Für die Remote-Administration von ViPNet Coordinator HW/VA kann das Applet ViPNet SGA verwendet werden, das eine komfortable Webschnittstelle zum Konfigurieren der Programmparameter bietet. Ausführliche Informationen über die Arbeit mit dem Applet ViPNet SGA sind im Dokument „ViPNet Coordinator HW/VA. Administratorhandbuch" enthalten.

- **Registrierung der Ereignisse in der Logdatei**

  Es besteht nun die Möglichkeit, Ereignisse, die während der Laufzeit der Software auftreten, in der System-Logdatei von ViPNet Coordinator HW/VA zu registrieren. Die in der Logdatei enthaltenen Daten können bei der Behebung möglicher Programmstörungen behilflich sein.

Glossar

B

Benutzerpasswort

Persönliches Passwort des Benutzers für die Anmeldung an seinem ViPNet Netzwerkknoten. Ursprünglich wird das Passwort im ViPNet Network Manager (in ViPNet VPN-Netzwerke) oder ViPNet Network Control Center (in ViPNet Netzwerke basierte auf der Software ViPNet Administrator) erstellt, kann aber durch den Benutzer geändert werden.

C

Coordinator (ViPNet Coordinator)

Ein Netzwerkknoten, auf dem die Software ViPNet Coordinator oder ViPNet Coordinator HW installiert ist. Ein ViPNet Coordinator funktioniert als ein Server innerhalb des ViPNet Netzwerks und leitet VPN-Traffic und Systemdaten weiter.

Siehe: Routing, ViPNet Netzwerk (auf S. 247).

D

Datei (Transportdatei)

Dienstinformation, die innerhalb des ViPNet Netzwerkes verwendet wird und durch das MFTP-Modul übermittelt wird.

DHCP (Dynamic Host Configuration Protocol)

Ein Netzwerkprotokoll der Anwendungsschicht, das es den Rechnern ermöglicht, IP-Adressen und andere für die Arbeit im TCP/IP-Netzwerk erforderlichen Parameter automatisch zu beziehen. Dazu zählen Parameter wie Subnetzmaske, Gateway-IP-Adresse, IP-Adressen der DNS Server, IP-Adressen der WINS Server.

DHCP-Server

Server, der die IP-Adressen der Clients automatisch verwaltet und entsprechende Einstellungen im Netzwerk durchführt.

DMZ (entmilitarisierte Zone)

Physikalisches oder logisches Subnetzwerk, das den Zugang aus dem umschließenden Netzwerk (normalerweise das Internet), zu dem kein Vertrauensverhältnis besteht, auf nach außen angebotene Dienste des Firmennetzwerks ermöglicht. Dabei befinden sich in diesem Subnetzwerk Server, die für Anfragen aus dem externen Netzwerk zuständig sind, und die durch Einsatz einer Firewall nur einen eingeschränkten Zugriff auf die Hauptsegmente des Firmennetzwerks haben. Eine direkte Verbindung zwischen dem internen und dem externen Netzwerk gibt es nicht: jede Verbindung wird über die Server in der DMZ aufgebaut, die eingehende Anfragen verarbeiten und eigene Anfragen generieren. Erhaltene Antworten werden von diesen Servern im eigenen Namen weitergeleitet.

DNS-Server

Server, der einen Teil der DNS-Datenbank verwaltet, die für den Zugriff auf Computernamen in der Internet-Domäne verwendet wird (Beispiel: ns.domain.net). In der Regel werden Domänendaten auf zwei DNS-Servern gespeichert, die als „Primary DNS“ und „Secondary DNS“ bezeichnet werden (die Duplizierung wird durchgeführt, um die Hochverfügbarkeit des Systems zu verbessern).

Der DNS-Server wird auch Domänennamenserver und Nameserver (DNS) genannt.

E

Externes Netzwerk

Das Netzwerk mit einem anderen IP-Adressen-Bereich im Vergleich mit dem lokalen Netzwerk. Normalerweise wird dieser Begriff für das Internet verwendet.

F

Firewall

Gerät oder Programm, das auf einem Netzwerkknoten an der Grenze des Netzwerks installiert ist, den gesamten ein- und ausgehenden IP-Traffic überprüft und Entscheidungen über die mögliche Weiterleitung des Traffics zu seinem Zielpunkt trifft. Das heißt, die Firewall dient der Verhinderung von unerlaubtem Zugriff von einem Netzwerk auf ein anderes. Die Firewall ist normalerweise für die Übersetzung der internen IP-Adressen in Adressen, auf die von einem externen Netzwerk aus zugegriffen werden kann, zuständig (Durchführung von NAT). In ViPNet werden drei Typen von Firewalls mit NAT unterschieden:

- ViPNet Coordinator – Modus, bei welchem als Firewall ein Computer mit installierter ViPNet Coordinator -Software auftritt, der NAT für verschlüsselten Traffic sicherstellt.
- Mit statischer Adressenübersetzung – Modus, bei dem zwischen dem geschützten Knoten und dem externen Netzwerk eine Firewall aufgestellt ist, die statische Umsetzung von IP-Adressen durchführt, d. h. die Interaktion externer Knoten mit einer bestimmten internen Netzwerkadresse über das UDP-Protokoll mit vorgegebenem Port sicherstellt.
- Mit dynamischer Adressenübersetzung – Modus, bei dem zwischen dem geschützten Knoten und dem externen Netzwerk eine Firewall aufgestellt ist, die dynamische Umsetzung von IP-Adressen durchführt. Dabei sollte im offenen Netzwerk ein Coordinator präsent sein, der die Verbindungen aufrechterhalten kann. Firewalls dieses Typs werden eingesetzt, wenn Verbindungen zum externen Netzwerk zum Beispiel über ein xDSL-Modem aufgebaut werden, das als Router auftritt, oder wenn dazu drahtlose Geräte, GPRS-Netze oder andere Anbieter, die private IP-Adressen zur Verfügung stellen, verwendet werden.

G

Geschützter Netzwerkknoten

Computer mit installierter ViPNet Software.

Grenze des lokalen Netzwerkes

Ein abstrakter Begriff, der einen Übergang von einem LAN in ein WAN oder in ein anderes LAN symbolisiert.

I

Internes Netzwerk

Lokales Netzwerk, für dessen Schutz eine VPN-Lösung vorgesehen ist.

IP-Adressenserver

Eine der Funktionen des ViPNet Coordinators. Ermöglicht die Registrierung und Vermittlung der Anschlussinformationen der Netzwerkknoten („online, „offline und Art des Internetanschlusses).

IPsec-Protokoll

Protokoll, das den Schutz des IP-Traffics durch Anwendung kryptografischer Methoden sicherstellt.

IP-Traffic

Datenfluss, der entsprechend den Regeln des IP-Protokolls über die Netzwerke übertragen wird.

L

Lizenzerweiterung für ViPNet VPN

Die Lizenzerweiterung bestimmt die Anzahl der Netzwerkknoten für bestimmte Anwendungen und Einzelkomponenten der ViPNet Produkte, die über die Größe eines Standardpaketes hinausgehen.

N

Netzwerkadressenübersetzung (NAT)

Network Address Translation ist der Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden.

Netzwerkfilter

Eine Zusammensetzung von Parametern, auf deren Basis die Firewall der ViPNet Software bestimmte IP-Pakete blockiert oder erlaubt.

Netzwerkknotenadministrator-Passwort

Das Passwort für die Anmeldung auf einem ViPNet Netzwerkknoten im Administratormodus. In diesem Modus stehen zusätzliche Konfigurationsmöglichkeiten für ViPNet Anwendungen zur Verfügung. Das Passwort des ViPNet Netzwerkknotenadministrators kann vom Administrator des ViPNet Netzwerks im Programm ViPNet Key and Certification Authority (ViPNet Netzwerke basierte auf der Software ViPNet Administrator) bzw. ViPNet Network Manager (ViPNet VPN-Netzwerke) erstellt werden.

Netzwerkprotokoll

Ein Netzwerkprotokoll ist eine Vereinbarung, nach der Daten zwischen Computern bzw. Prozessen ausgetauscht werden, die durch ein Netz miteinander verbunden sind.

NTP-Server

Server der genauen Uhrzeit, der dafür zuständig ist, die Systemzeit der Computer, Arbeitsstationen, Server und anderer Netzwerkgeräte zu synchronisieren. Dieser Server tritt als Vermittler zwischen dem Referenzzeitgeber und dem lokalen Netzwerk auf. Er erhält die genaue Zeit vom Referenzzeitgeber über einen speziellen Verbindungskanal (Schnittstelle) und leitet die Daten an jeden Netzwerkknoten weiter. Dadurch wird die Synchronisation der Geräte untereinander sichergestellt.

O

Offener Netzwerkknoten

Ein Netzwerkobjekt ohne ViPNet Software.

S

Schlüsseldistribution

Die Datei mit der Erweiterung `.dst`, wird im ViPNet Network Manager (in ViPNet VPN-Netzwerke) oder ViPNet Network Control Center (in ViPNet Netzwerke basierte auf der Software ViPNet Administrator) erstellt. Die Datei beinhaltet Schlüsselinformationen, Adresslisten und die Lizenzdatei, die für den initialen Start des Netzwerkknotens erforderlich sind.

Schlüsselupdate

Bei der Veränderung der logischen Struktur des ViPNet Netzwerkes werden die Schlüssel sowie die Adressenlisten der betroffenen Netzwerkknoten geändert. In diesem Falle ist eine Aktualisierung der o.g. Informationen notwendig. Diese Aktualisierungen werden vom ViPNet Network Manager oder dem ViPNet Network Control Center versendet.

Subnetzmaske

Die Netzmaske, Netzwerkmaske oder Subnetzmaske ist eine Bitmaske, die im Netzwerkprotokoll IPv4 bei der Beschreibung von IP-Netzen angibt, wie viele Bits am Anfang der dargestellten IP-Adresse das Netzpräfix ausmachen.

T

Trunk

In der Terminologie der Telekommunikation wird ein Übertragungskanal zwischen zwei Telekommunikationsroutern (z. B. VoIP-Servern) als Trunk bezeichnet. Eine Trunk-Verbindung ermöglicht es den Netzwerkbenutzern, Clients hinter dem Datenrouter eines anderen Telekommunikationsnetzwerks anzurufen.

Tunnelung

Verschlüsselung des Traffics der offenen Netzwerkobjekte bei der Übertragung über öffentliche Netzwerke.

V

ViPNet Network Manager

Verwaltungsmodul aus dem Paket ViPNet VPN, dient zum Erstellen und Verwalten kleiner und mittlerer ViPNet Netzwerke.

ViPNet Netzwerk

Mit Hilfe von ViPNet Software aufgebautes logisches Netzwerk.

ViPNet Netzwerkknoten

Computer mit installierter ViPNet Software.

ViPNet VPN Lizenz

Die Lizenz bestimmt die Netzwerknummer, die Anzahl der Netzwerkknoten für bestimmte Anwendungen und Einzelkomponenten der ViPNet Produkte, die maximal erlaubte Version der Software, die Laufzeit der Software und andere Parameter.

Virtuelle IP-Adresse

Die virtuelle IP-Adresse wird auf einem ViPNet Netzwerkknoten für die Gegenstelle generiert und ist an die ID-Nummer der Gegenstelle gebunden. Die Verwendung der virtuellen IP-Adressen ermöglicht es, IP-Adressen-Überschneidungskonflikte zu vermeiden und die reelle Topologie des Netzwerkes zu kaschieren.

Virtuelles Privates Netzwerk (VPN)

Das konventionelle VPN dient dazu, Teilnehmer eines Netzes (auch mobile Benutzer) aus ihrem ursprünglichen Netz heraus an ein anderes Netz anzubinden. Diese Anbindung erfolgt

üblicherweise über öffentliche Netze unter Verwendung von Verschlüsselungs- und Authentisierungsmechanismen.

Index

Z